

IN THE COURT OF APPEAL OF THE STATE OF CALIFORNIA
FOURTH APPELLATE DISTRICT, DIVISION ONE

THE PEOPLE OF THE STATE OF CALIFORNIA,

Plaintiff and Respondent,

v.

KEVIN CHRISTOPHER BOLLAERT,

Defendant and Appellant.

Case No. D067863

San Diego County Superior Court, Case No. SCD252338
The Honorable David M. Gill, Judge

RESPONDENT'S BRIEF

KAMALA D. HARRIS
Attorney General of California
GERALD A. ENGLER
Chief Assistant Attorney General
JULIE L. GARLAND
Senior Assistant Attorney General
ERIC A. SWENSON
Supervising Deputy Attorney General
JUNICHI P. SEMITSU
Deputy Attorney General
GARRETT A. GORLITSKY
Deputy Attorney General
STEVE OETTING
Deputy Solicitor General
State Bar No. 142868
600 West Broadway, Suite 1800
San Diego, CA 92101
P.O. Box 85266
San Diego, CA 92186-5266
Telephone: (619) 645-2206
Fax: (619) 645-2012
E-mail: Steve.Oetting@doj.ca.gov
Attorneys for Plaintiff and Respondent

TABLE OF CONTENTS

	Page
Introduction	1
Statement of the Case.....	3
Statement of Facts.....	4
Argument.....	20
I. Appellant was an “information content provider,” or alternatively acted with an intent to defraud, and therefore he was not immune to prosecution for identity theft; further, substantial evidence supports his convictions	20
A. Applicable law.....	21
B. Appellant was an information content provider and therefore fell outside the exclusion of Penal Code section 530.5, subdivision (f).....	25
C. Appellant retained possession of personal identifying information with the intent to defraud the victims	32
D. There was no First Amendment violation.....	34
E. Appellant willfully obtained personal identifying information	34
F. Appellant used the personal identifying information for an unlawful purpose	35
1. Section 653m	35
2. Intrusion into private affairs	37
3. Public disclosure of private facts.....	41
4. Any error was harmless.....	42
II. Substantial evidence supports appellant’s convictions for extortion.....	42
III. Appellant invited any error regarding the CACI instructions he requested; in any event, the instructions, when construed as a whole, required the jury to determine every element beyond a reasonable doubt	53
Conclusion.....	61

TABLE OF AUTHORITIES

	Page
CASES	
<i>Barnes v. Yahoo! Inc.</i> (9th Cir. 2009) 570 F.3d 1096.....	28
<i>Barrett v. Rosenthal</i> (2006) 40 Cal.4th 33.....	22
<i>Batzel v. Smith</i> (9th Cir. 2003) 333 F.3d 1018.....	26, 28
<i>Boyde v. California</i> (1990) 494 U.S. 370	55
<i>Brown v. Payton</i> (2005) 544 U.S. 133	55
<i>Carafano v. Metrosplach.com, Inc.</i> (9th Cir. 2003) 339 F.3d 1119.....	26, 27, 28, 31
<i>Chicago Lawyers' Comm. For Civil Rights Under Law, Inc.</i> <i>v. Craigslist, Inc.</i> (7th Cir. 2008) 519 F.3d 666	22
<i>Cross v. Cooper</i> (2011) 197 Cal.App.4th 357	44, 48, 49
<i>Diaz v. Oakland Tribune, Inc.</i> (1983) 139 Cal.App.3d 118	41
<i>Dietemann v. Time, Inc.</i> (9th Cir. 1971) 449 F.2d 245	40
<i>Doe II v. MySpace Inc.</i> (2009) 175 Cal.App.4th 561	28
<i>Doe v. GTE Corp.</i> (7th Cir. 2003) 347 F.3d 655	22

TABLE OF AUTHORITIES
(continued)

	Page
<i>F.T.C. v. Accusearch Inc.</i> (10th Cir. 2009) 570 F.3d 1187.....	23, 30
<i>Fair Housing Council of San Fernando Valley v. Roommates.Com, LLC</i> (9th Cir. 2008) 521 F.3d 1157.....	<i>passim</i>
<i>Flatley v. Mauro</i> (2006) 39 Cal.4th 299	34, 52
<i>Four Navy SEALs v. Associated Press</i> (S.D. Cal. 2005) 413 F.Supp.2d 1136	40, 41
<i>Giboney v. Empire Storage & Ice Co.</i> (1949) 336 U.S. 490	34
<i>Howard Contracting, Inc. v. G.A. MacDonald Construction Co.</i> (1998) 71 Cal.App.4th 38	52
<i>In re Rolando S.</i> (2011) 197 Cal.App.4th 936	35, 37, 59, 60
<i>Jackson v. Virginia</i> (1979) 443 U.S. 307	21
<i>Jones v. Dirty World Entertainment Recordings, LLC</i> (6th Cir. 2014) 755 F.3d 398	29, 30
<i>Korea Supply Co. v. Lockheed Martin Corp.</i> (2003) 29 Cal.4th 1134.....	59
<i>Leser v. Penido</i> (2009) 879 N.Y.S.2d 107.....	45
<i>Levitt v. Yelp! Inc.</i> (9th Cir. 2014) 765 F.3d 1123 (<i>Yelp!</i>).....	50, 51, 52, 53
<i>Melvin v. Reid</i> (1931) 112 Cal.App. 285	42, 49

TABLE OF AUTHORITIES
(continued)

	Page
<i>People v. Barba</i> (2012) 211 Cal.App.4th 214	2
<i>People v. Booth</i> (1996) 48 Cal.App.4th 1247	32
<i>People v. Cain</i> (1995) 10 Cal.4th 1.....	55
<i>People v. Castillo</i> (1997) 16 Cal.4th 1009.....	55
<i>People v. Choynski</i> (1892) 95 Cal. 640.....	44
<i>People v. Crittenden</i> (1994) 9 Cal.4th 83.....	52
<i>People v. Gionis</i> (1995) 9 Cal.4th 1196.....	34
<i>People v. Guiton</i> (1993) 4 Cal.4th 1116.....	42, 53
<i>People v. Jenkins</i> (1994) 29 Cal.App.4th 287	55
<i>People v. Kelly</i> (1992) 1 Cal.4th 495.....	55
<i>People v. Kraft</i> (2000) 23 Cal.4th 978.....	21, 49
<i>People v. Lavine</i> (1931) 115 Cal.App. 289	47
<i>People v. Lucero</i> (2000) 23 Cal.4th 692.....	54

TABLE OF AUTHORITIES
(continued)

	Page
<i>People v. Massengale</i> (1968) 261 Cal.App.2d 758	44, 45
<i>People v. Mills</i> (1991) 1 Cal.App.4th 898	55
<i>People v. Oppenheimer</i> (1962) 209 Cal.App.2d 413	44, 45, 49
<i>People v. Peniston</i> (1966) 242 Cal.App.2d 719	47, 48, 51, 52
<i>People v. Price</i> (1991) 1 Cal.4th 324.....	55
<i>People v. Reed</i> (1961) 190 Cal.App.2d 344	33
<i>People v. Seaton</i> (2001) 26 Cal.4th 598.....	54
<i>People v. Snow</i> (2003) 30 Cal.4th 43.....	21
<i>People v. Turner</i> (2004) 34 Cal.4th 406.....	54
<i>People v. Van Winkle</i> (1999) 75 Cal.App.4th 133	55
<i>People v. Weaver</i> (2001) 26 Cal.4th 876.....	54
<i>Philippine Export & Foreign Loan Guarantee Corp.</i> <i>v. Chuidian</i> (1990) 218 Cal.App.3d 1058	52
<i>R.A.V. v. City of St. Paul</i> (1992) 505 U.S. 377	34

TABLE OF AUTHORITIES
(continued)

	Page
<i>Rejent v. Liberation Publications, Inc.</i> (1994) 611 N.Y.S.2d 866.....	45
<i>Sanders v. American Broadcasting Cos.</i> (1999) 20 Cal.4th 907 (<i>Sanders</i>).....	39, 40, 41, 59
<i>Shulman v. Group W Productions, Inc.</i> (1998) 18 Cal.4th 200.....	38, 41
<i>United States v. Lifshitz</i> (2d Cir. 2004) 369 F.3d 173.....	40
<i>United States v. Quinn</i> (5th Cir. 1975) 514 F.2d 1250.....	34
<i>Universal Communication Systems, Inc. v. Lycos, Inc.</i> (1st Cir. 2007) 478 F.3d 413.....	28
<i>Zeran v. America Online, Inc.</i> (4th Cir. 1997) 129 F.3d 327	24, 28
 STATUTES	
United States Code, Title 47	
§ 230(b)(5)	24
§ 230(c)	24
§ 230(c)(1).....	23
§ 230(d)(1)	24
§ 230(d)(3)	24
§ 230(f)	2
§ 230(f)(2)	22
§ 230(f)(3).....	23, 26
 Code of Civil Procedure	
§ 425.16	48
Communications Decency Act (CDA)	<i>passim</i>
 Digital Millennium Copyright Act (DMCA),	
17 U.S.C. § 512(c).....	9, 15, 16, 17

TABLE OF AUTHORITIES
(continued)

	Page
Hobbs Act	
(18 U.S.C. § 1951(b)(2)).....	51
Penal Code	
§ 7, subd. (1).....	35
§ 123	43
§ 182, subd. (a)(1)	3
§ 518	43, 51
§ 519	43, 45, 51
§ 519, subd. (1).....	50, 51
§ 519, subd. (3).....	45, 49, 51
§ 519, subd. (4).....	45, 51
§ 520	2, 3
§ 523	45
§ 530.5	<i>passim</i>
§ 530.5, subd. (a).....	<i>passim</i>
§ 530.5, subd. (f)	<i>passim</i>
§ 530.55	52
§ 530.55, subd. (b).....	21, 28
§ 653m	<i>passim</i>
§ 653m, subd. (a).....	35, 36
§ 654	4
§ 1118.1	3
§ 1170, subd. (h).....	4
 CONSTITUTIONAL PROVISIONS	
United States Constitution	
First Amendment.....	34
 OTHER AUTHORITIES	
5 Witkin Summary of California Law,	
Torts, § 658 p. 963.....	38

INTRODUCTION

Appellant Kevin Bollaert operated a website called “UGotPosted.com,” which encouraged users to post private, intimate photographs of others. As the very name of appellant’s website—UGotPosted—suggests, it was intended to notify victims that someone else had posted pictures of them without the victims’ consent. In order to post such pictures, the website required the poster to include personal identifying information of the person depicted, including that person’s full name, city of residence, and Facebook profile link. Typically, the posters were scorned lovers who obtained the photographs before the relationship soured and then posted them on appellant’s website without the victims’ consent; in other cases photographs were taken of victims while they were unaware or incapacitated, and sometimes the photos were stolen from the victims. Appellant relied on other Internet users to see the postings and contact the victims using the victims’ posted identifying information. For many of the victims, the results were disastrous. Some of the victims received hundreds of unwanted and sometimes threatening contacts, resulting in humiliation, social ostracization, and even loss of employment. Many victims understandably suffered deep depression, and at least one even attempted to take her own life.

Appellant’s intent in operating the website was to extort money from the victims in exchange for removing the damaging photos and identifying information. Shamed, harassed and embarrassed, the victims would invariably seek to have the photographs taken down. When the victims appealed to appellant’s website to remove the photos, they were often directed to another website appellant operated called “ChangeMyReputation.com.” On that website, appellant would agree to remove the photographs in exchange for a payment via PayPal or Amazon gift card. And many desperate victims paid.

Appellant was convicted of multiple counts of unauthorized use of personal identifying information (Pen. Code, § 530.5, subd. (a))¹—commonly referred to as “identity theft”²—and extortion (§ 520). The crime of identity theft requires use of personal identifying information for an unlawful purpose. The prosecution proceeded on three separate theories to establish appellant’s unlawful purpose, based on violations of section 653m (contact by electronic communication with intent to annoy), public disclosure of private facts, and intrusion into private affairs. The jury returned special findings demonstrating which of the theories they relied upon for each count.

Appellant now appeals, claiming there was insufficient evidence to support his conviction under section 530.5 because he fell within an exception under the Communications Decency Act (CDA), 47 United States Code section 230(f), for “interactive service providers” or “access software providers,” and he was not an “information content provider.” But appellant is mistaken. By requiring users to post personal identifying information, appellant became an “information content provider” because he was responsible as a developer and provider of the content he required; thus, he was no longer a mere “interactive service provider” or “access software provider”. In any event, because he intended to defraud victims by concealing his true identity as the operator of both websites, the exception appellant relies on would not apply. Further, there was more than ample evidence that appellant willfully committed identity theft by possessing the victims’ personal identifying information for a variety of unlawful reasons.

¹ All further references are to the Penal Code, unless otherwise noted.

² Although commonly referred to as “identity theft,” as this Court has pointed out, nothing in section 530.5 refers to that term. (*People v. Barba* (2012) 211 Cal.App.4th 214, 226.)

Appellant also challenges the sufficiency of the evidence to support the extortion charges. According to appellant, he did nothing more than engage in “standard business practice.” But the evidence demonstrates he committed extortion by threatening the continued exposure of the victims’ naked photos unless they paid to have those photos removed.

Finally, appellant argues that the trial court’s instructions that allowed the jury to convict him of an unlawful purpose to commit identity theft based on a tortious invasion of the right to privacy lowered the burden of proof to a civil preponderance of the evidence standard. Appellant is incorrect. The court’s instructions, which appellant requested, unambiguously required proof beyond a reasonable doubt. While the instructions correctly noted that tortious invasions of the right to privacy could constitute an unlawful purpose, that intent to commit a tortious act still had to be proved beyond a reasonable doubt. Accordingly, the judgment should be affirmed.

STATEMENT OF THE CASE

The California Attorney General’s Office filed an amended information in the San Diego County Superior Court charging appellant with one count of conspiracy to commit identity theft (§§ 182, subd. (a)(1), 530.5, subd. (a)), nine counts of extortion (§ 520), and 26 counts of identity theft. (1CT 164-175.)

Appellant pleaded not guilty and proceeded to trial by jury. (1RT 8.) At the conclusion of the People’s case-in-chief, the trial court granted appellant’s motion to dismiss four counts of identity theft and three counts of extortion, and renumbered the remaining counts. (1CT 164-175.) The court otherwise denied appellant’s motion to dismiss the remaining counts under section 1118.1. (7RT 906-950.)

The jury found appellant guilty of 6 counts of extortion and 21 counts of identity theft. (3CT 724-771.) The jury deadlocked as to the conspiracy

charge (count 1) and one count of identity theft (count 25), and the court declared a mistrial as to those counts. (3CT 772.) The prosecution proceeded on three separate theories of identity theft and the jury was asked, to the extent it was unanimous, to make special findings as to which of these theories was true. As to renumbered counts 2, 4-6, 8-15, 19, 23, and 26, the jury found that appellant committed an unlawful act of invasion of privacy by disclosure of private facts. (3CT 724-725, 727-732, 735-750, 755-756, 762-763, 766-767.) For counts 7, 17, 20, 22, 24, and 28 the jury did not return any special finding. (3CT 733-734, 752-753, 757-758, 760-761, 764-765, 769-770.)

The court initially sentenced appellant on April 3, 2015, to a total term of 18 years in jail, comprised of a middle 3-year term for count 3 and one-third the midterm (i.e., 8 months for the identity theft counts and 1 year for the extortion counts) consecutive for each of the remaining counts, with the exception of counts 2, 15, 17, 26, 28, which the court stayed under section 654. (9RT 1644-1653; 3CT 773-777.)

Appellant filed a notice of appeal from the judgment on April 13, 2015. (3CT 646.)

However, the court recalled the sentence and resentenced appellant on September 21, 2015. At that time, the trial court again imposed an 18-year term, but determined the sentence would be “split” under section 1170, subdivision (h), to provide for eight years of local confinement followed by ten years of mandatory supervision. (9/21/15 RT at 91.)

STATEMENT OF FACTS³

The California Attorney General's Office became aware of the UGotPosted.com website around October 2012, and opened an investigation. (7RT 857-858.) The site contained naked photos of men and women, as well as an opportunity for commentators to post remarks about the photos. (7RT 859.) Many, but not all, of the persons depicted in the photos were from California. (7RT 858.) The UGotPosted site was configured with a banner at the top of the page; beneath this was a disclaimer; the photos for a particular individual came next; and finally, under the photos were the specific comments for that individual. On the right hand side of the page was a navigation bar; on the bottom was a link to contact the administrator. (5RT 448-449.) The administrator, who had the ability to select photos that were posted, create descriptive content and text, and moderate comments, had to approve comments before they were published. (5RT 488.) The site could be searched based on name or geographic location of the persons who were posted. (5RT 456; 7RT 864.) As designed, the UGotPosted site required posters to provide information in several fields before they could submit anything. These required fields included the following: 1. The email address of the submitter; 2. The full name of the person posted; 3. The location of the person posted, including the city, county and state; 4. The age of the person posted (who was nominally required to be over 18); 5. Facebook links to the posted person's page; 6. The poster's agreement to the conditions of use; and 7. Photos. (5RT 452-454, 509-510, 525.)⁴

³ This Statement of Facts omits testimony relating to the counts on which the jury hung, as well as testimony regarding an additional uncharged offense.

⁴ Appellant asserts that the site "asked for, but did not demand, Facebook information." (AOB 17.) That is incorrect. Providing a

(continued...)

After determining that appellant was the registered owner of UGotPosted.com and that he operated the site in San Diego, Special Agent Brian Cardwell of the Department of Justice eCrimes Unit arranged a meeting with him at a hotel lobby on September 18, 2013. (6RT 782, 785, 790-791; ex. 1.) During the meeting, which Special Agent Cardwell surreptitiously recorded (exs. 1, 3), appellant admitted owning and designing the site, which required users to post a full name, date of birth, location and Facebook link.⁵ (2CT 289.) According to appellant, he created the site because it was “fun and entertaining.” (2CT 292.) He started the site roughly a year earlier with Eric Chanson; Chanson declined to participate after December 2012 and so he agreed to transfer the ownership rights to appellant. (2CT 292, 297, 299.) During the year of its operation, appellant received approximately 10,000 posts, and he personally examined each one. (2CT 299-300.)⁶ Appellant would not post submissions that did not include nude photos, and he would place a proprietary watermark on all photos to prevent theft by another website. (2CT 298-299.) Appellant denied making any significant money from the site. (2CT 290.) Although the site provided his sole source of employment, according to appellant he received only \$900 a month from advertising. (2CT 303.) Ultimately, appellant decided to take the site down because it was too much “stress,” and was “ruining [his] life.” (2CT 287, 292.) At the end of the interview,

(...continued)

Facebook link was a required field; other additional information, such as a Tumblr or Twitter account was optional. (5RT 493-494.)

⁵ Appellant maintained that a poster could provide a fake name and Facebook link. (2CT 289.) However, appellant apparently verified the postee’s identity, going onto victims’ Facebook pages to view photographs on 2,300 separate occasions. (5RT 493-494.)

⁶ Exhibit 14 contains one page from the list of 10,000 victims. (5RT 390.)

appellant provided the encryption codes for several of his laptops so that Agent Cardwell could copy the hard drives. (6RT 818.) A subsequent examination of appellant's email accounts revealed that the majority of 2,500 emails sent to appellant consisted of requests to have images removed from his site. (6RT 841.)

Forensic computer expert Mark Kelly conducted a forensic examination of appellant's primary computer. (5RT 380-381.) Kelly determined that appellant was the website administrator, or the person in control over the website, and he had the only user account on the computer. (5RT 394-395, 422.) The administrator had to review and approve each submission before it could be posted. (5RT 396, 526.)⁷ Appellant's online moniker was "Vindictive2786". (5RT 433.) Some of the documents captured from his computer included conversations between appellant and Chanson regarding the design of the website. (5RT 433, 436.) In one such exchange, appellant stated that he was in control of the website and he made the decisions. (5RT 436; ex. 46.) They also discussed removing photos only in exchange for payment. (5RT 438.) When someone would send appellant a request to have images removed, appellant would direct that person to a separate website he set up, ChangeMyReputation.com, to pay; once the person paid, the information was removed. (5RT 439; ex. 79 [examples of emails in which this occurred].)

A forensic audit revealed that the website received over \$30,000 in payments via PayPal. (7RT 894; ex. 87.) The Attorney General's Office used the contact information on the website to reach out to victims. (7RT 859.)

⁷ At one point the Attorney General's Office attempted to submit photos of cats, rather than naked humans, to determine whether the website administrator was actively reviewing the photos before they were posted; the photos of the cats were never posted. (7RT 860-861.)

Counts 2 and 3: Identity theft and extortion of Rebecca.

Rebecca awoke one morning in March 2013 to find that she had six missed calls from her manager and had received roughly 300 Facebook messages from strangers. (6RT 627, 629; exs. 41, 62.) She discovered that intimate, naked photos of herself and her ex-fiancée were posted on the UGotPosted site, along with her full name, work location, Facebook link and age. (6RT 629.) Her fiancée had taken the pictures about a year earlier, before they broke up. (6RT 637.) Someone had contacted her manager at work and let him know that Rebecca was doing “suspicious activity on the Internet.” (6RT 627.) Hurt and embarrassed, Rebecca felt that she had become an involuntary “pornography star” and she was afraid that her seven-year-old son would learn of the postings. (6RT 638.)

Rebecca emailed the website, demanding that the photos be taken down, but she did not receive a response. (6RT 632-633, 636.) Based on a link she found on the UGotPosted site, she also emailed ChangeMyReputation.com. She received a response from the latter email within a few minutes, directing her to pay \$249.99 via PayPal. (6RT 633-636.) Rebecca paid the money because she felt the pictures were disgusting, and also because the nude photos were the first images that appeared when she Googled her name. (6RT 635-636.) Although she knew some people had already seen the images, she paid so that other people would not. (6RT 639.)

Count 4: Identity theft of Brianna

In October 2013, strangers began contacting Brianna on Facebook, informing her that her photographs had been posted on UGotPosted.com. (4RT 268; ex. 76.) Some of the strangers solicited her for sex, others generally harassed her. (4RT 273.) Some people called her work and tried to get her fired. (4RT 273.) Brianna went on the website and saw naked photos of herself, which were taken without her knowledge by a former

boyfriend and were posted without her consent. (4RT 270-273, 275.) Other clothed photos that she had posted on Facebook were also on the UGotPosted site, again without her consent. (4RT 270.) Brianna sank into depression as a result of the experience and did not want to see anyone or go anywhere. (4RT 273.) She contacted the website, asking to have the photos removed, but no one responded to her emails. (4RT 272, 276.)

Count 5: Identity theft of Jane Doe

In May 2013, Jane Doe began receiving explicit and vulgar messages from men. (5RT 605.) She found her images were posted on several websites, including UGotPosted. (5RT 606; ex. 1, 18.) That website included many photos of her, as well as the name of the law school she was attending, her Facebook page, telephone number, and Instagram and Twitter accounts. (5RT 606, 511.) Jane had sent the pictures to her boyfriend, who in turn posted them without her consent. (5RT 608.)

Some of the comments discussed plans to rape Jane; other comments addressed her promiscuity. (5RT 609.) Because one of the comments suggested that she was sleeping with her professors, she was ultimately contacted by school administrators and was forced to endure an honor board investigation and hearing. (5RT 606-607.)

Jane worked with an FBI agent, but was unsuccessful in having her photos removed. She hired an attorney, who contacted UGotPosted and was able to have the photos removed after another two weeks, but only after Jane had her photos copyrighted and filed a complaint under the Digital Millennium Copyright Act (DMCA), 17 U.S.C. § 512(c). (5RT 610, 614.)

The subject of the photos came up frequently when Jane interviewed for employment with various law firms; she did not receive any offers. (5RT 607-608.) Jane spent her days crying; at night, she would fall asleep holding a can of pepper spray. (5RT 606.) Afraid that she would be raped,

Jane did not leave her house unless absolutely necessary. (5RT 609.)
Eventually, she went to therapy. (5RT 606.)

Count 6: Identity theft of V.

In July 2013, V. became aware that photos of her had been posted on UGotPosted when she began receiving “nonstop” text messages and “hundreds” of Facebook comments from strangers. (6RT 771-772, 774-775.) She discovered that naked photos of her were published on the site, along with her full name, and Facebook and Twitter links. (6RT 773; ex. 77.) Commentators on the site made racist and vulgar remarks. (6RT 774.) She presumed that her former boyfriend must have taken the pictures while she was unaware; she did not consent to have them taken or posted. (6RT 771.) V. was forced to have her phone disconnected, and she either shut down her social media or changed the privacy settings. (6RT 772.) When her friends found out about the photos, she became withdrawn and isolated. (6RT 773-774.) At the time, she was looking for a job, and so she was forced to give up her search, knowing that any future employer would likely Google her name, which is unique. (6RT 773.) She wrote three to five emails to the website and eventually the photos were removed. (6RT 775.)

Count 7: Identity theft of Alice

While at a party in August 2013, someone drugged Alice’s drink. She woke up the next morning without any memory of what had occurred. (4RT 277-278.) A few days later, Alice began receiving messages from strangers saying she had been “posted.” (4RT 278.) She went on the UGotPosted website and saw naked pictures of herself, taken while she was incapacitated and placed in compromising positions, as well as her address. (4RT 280, 282; ex. 75.) Other pictures depicted her clothed and were taken from her Facebook site. (4RT 281.) Comments on the website frightened her. (4RT 283.) She did not give anyone permission to post any of her

photos. (4RT 281.) Alice sent an email to the website asking to have the photos removed, but the response said she would have to pay. (4RT 283.) As a result of the posting, she lost friends; someone notified her employer; and she received harassing messages telling her to kill herself. (4RT 284.)

Count 8: Identity theft of Nina

In August 2013, Nina's father, a police officer, notified her that photos of her had been posted on UGotPosted.com. (5RT 399.) She discovered that naked pictures of her had been posted along with her full name, Facebook page, city and state. (5RT 400, 403; ex. 78.) A profile picture had also been "stolen" from her Facebook page. (5RT 402.) She had originally sent the naked photos to a friend from high school, and later asked him to delete them. (5RT 404-405.) Nina emailed the website, asking it to remove the pictures, and giving notice that the photos were posted without her consent and that a police report had been filed, but she received no response. (5RT 404.) The website led her to ChangeMyReputation.com, which promised to remove the photos for \$500, but Nina decided not to pay. (5RT 404.) As a result of the posting, Nina received lewd messages from strangers. She felt violated and threatened. (5RT 405-406.) Her children and other family members learned of the pictures, causing further embarrassment. (5RT 407.)

Count 9: Identity theft of Kaye

In August 2013, Kaye received roughly 50 messages indicating that her photos were on UGotPosted. (6RT 679.) When she checked the website, she discovered that in addition to her photos, the site also had her Twitter account, her Facebook link, her full name, and her town. (6RT 680, ex. 61.) She had sent the photos to a boy who took her to the prom, making it clear that they were intended to be kept confidential. (6RT 687.) He later threatened to put the photos up on the Internet when Kaye refused to speak with him. (6RT 690.)

In the website's comments section, posters discussed her bodily attributes. (6RT 680.) Kaye was frightened because her location was posted. She felt that she could not use social media. (6RT 681.) She notified the website that she was underage at the time the photos were taken, and demanded that they be taken down. (6RT 684.) A detective also contacted the website, but the images were never removed. (6RT 686.)

Count 10: Identity theft of Nicole C.

In May 2013, Nicole C.'s Facebook page was bombarded with hundreds of lewd messages from strangers. (4RT 290.) She discovered that naked photos, which she had taken of herself for her fiancée, had been posted without her consent along with her Facebook address, home address and telephone number. (4RT 291, 293; ex. 60.) She went to the police, and the photos were temporarily taken down, but then were later reposted. (4RT 293.) As a result of the postings, she tried to take her life and eventually wound up in a psychiatric hospital. (4RT 294.)

Count 11: Identity theft of Sarah

In May 2013, Sarah received roughly 30 Facebook messages indicating that naked photos of her had been posted online. (5RT 537-538.) She went to the UGotPosted website and saw naked photos of herself, along with her Facebook link, her full name and her city. (5RT 538-539; ex. 64.) She had taken the photos of herself with a webcam, but she had not sent them to anyone and believed that her computer had been hacked. (5RT 544, 546.)⁸ Commentators on the site discussed her weight, suggesting she ate out of a trough or stating, "suey, pig, pig, pig." (5RT 539.) Sarah emailed the site administrator and asked that her photos be removed.

⁸ Sarah had previously told an investigator with the Attorney General's Office that she had sent the photos to her ex-boyfriend plus ten others. 8RT 1046.)

Although the photos were removed, a different set of photos was later re-posted. (5RT 538, 543, 548.) The results of the posting were “devastating,” damaging Sarah’s self-esteem and making her paranoid of others. (5RT 539.) Because she lived in a small town, she lived in fear that someone would find out about the site. (5RT 540, 544, 550.) She blocked her privacy settings in the hope that her family would not find out. (5RT 548-549.) However, she felt that she was not able to apply for any job because any Google search of her name would reveal the photos. (5RT 545.)

Count 12: Identity theft of Brittany B.

One morning in July 2013, Brittany awoke to nearly 300 Facebook messages. (4RT 349.) She discovered naked photos of herself, along with her age and a link to her Facebook profile, posted without her consent on the UGotPosted site. (4RT 350, 352; ex. 5.) She had sent the naked pictures to a former boyfriend, who was deployed in Iraq at the time. (4RT 351.) Some of the comments she received were racist, others discussed the fact that she had subsequently become pregnant and speculated as to the circumstances. (4RT 354.) Brittany sent five or six emails to the website requesting that the photos be removed, but she received no response. (4RT 354, 356.) Brittany was humiliated, and was forced to explain the circumstances behind the photos to both her husband and her husband’s family. (4RT 349, 356.)

Count 13: Identity theft of Megan B.

In January 2013, Megan took some selfies of herself while naked, and sent them to her boyfriend and a long-time friend. (4RT 318-319.) Sometime after that, she began receiving vulgar messages on Facebook indicating that she had been posted. (4RT 319; ex. 48.) She discovered that the naked photos of herself had been posted on the UGotPosted site without her consent. (4RT 319.) Comments on the site referred to her as a “nasty,” “tattooed,” “mixed breed.” (4RT 324.) Scared, angry and frightened,

Megan went on the UGotPosted website and asked that the pictures be taken down. (4RT 320, 322.) She communicated with someone who referred to himself as “James Smith,” not realizing it was really appellant. (4RT 324-325.) He told her that to have the pictures removed, she would have to provide two forms of identification, and take a picture while holding a sign. (4RT 325; ex. 49.) Megan did as required, but the photos were still not removed. (4RT 325.)

Count 14: Identity theft of Christina

In 2013, someone with a fake profile sent Christina a message on her Facebook page, threatening to expose nude pictures of her if she did not send him money. (6RT 644.) At some later point, she received a message with a link to the UGotPosted website. When she clicked on the link, she saw graphic photos of herself. (6RT 645-646; ex. 52.) She had previously taken the photos of herself, and they were on her phone when it was stolen. (6RT 648.) Her name, hometown, and Facebook profile were also listed on the website. (6RT 646.) She believed it was the thief who posted both her photos and her information. (6RT 650.) She emailed UGotPosted and informed the site that she was only 17 at the time the photos were taken. (6RT 647.) Christina also contacted the police, but she never heard of any follow-up. (6RT 651.)

The exposure “ruined [her] life.” (6RT 646.) Christina’s family no longer accepted her, and she lost friends. (6RT 646, 648.) Believing Christina had brought shame on the family, her mother even tried to beat her up. (6RT 647.) She was kicked out of her family’s house and became homeless. With her reputation in disgrace, it was hard to find a job. Although she finally found a job a few weeks before she testified, she was not sure how long it would last. (6RT 647.) Because she lived in a small town, it was hard for her to even walk around in public. (6RT 648.)

Counts 15 and 16: Identity theft and extortion of Jennifer

In late 2012 or early 2013, Jennifer received a dozen or more Facebook messages indicating that photos of her were posted on the UGotPosted site, or otherwise discussing her body parts. (5RT 594.) Afraid that she was being stalked, she went to the website. There, she discovered both naked and clothed pictures of herself, as well as her full name, Facebook link, email address, location and employer. (5RT 595-596; ex. 36.) She had sent the naked pictures to her then-boyfriend (5RT 600); the clothed pictures came from her Facebook page (5RT 596). She did not give anyone permission to use any of the photos. (5RT 596, 601.) Commentators made racial slurs, picked apart her body, and discussed how disgusting she was. (5RT 596.) It made her feel “horrible,” “dirty,” and “terrified.” (5RT 596.) Jennifer emailed the website and asked that her photos be taken down. (5RT 598.) She was directed to ChangeMyReputation.com, which in turn required her to pay \$249.99 to have the photos removed. (5RT 600.) That website informed her that if she did not pay, the photos would remain up. (5RT 602.) Jennifer made the payment as required, and the photos were removed. (5RT 601.) She decided to pay the money because the postings were affecting her work and social life, and she did not want anyone else to see the photos. (5RT 603.)

Counts 17 and 18: Identity theft and extortion of Alaina

In May 2013, Alaina received a call at work from a stranger who notified her that she had been posted. Checking the UGotPosted site, she discovered naked pictures of herself that she had originally posted on her own personal blog. (4RT 299; ex. 54.) Her blog did not use her actual name or identifying information. (4RT 205.) However, the UGotPosted website included not only her full name, age, and city, but also the school from which she had graduated. (4RT 303.) She notified the UGotPosted website that her photos were copyright-protected under the DMCA, but she

received no response. Alaina also falsely told the website that she was under 18 when the photos were taken, but again she received no response. (4RT 298.) Finally, she decided to pay a \$350 “blackmail fee” to “ChangeMyReputation.com” because it was linked to the website and it represented it would take the photos down with payment. (4RT 298, 302.) As a result of the posting, Alaina suffered psychological trauma. She was afraid she was being stalked and so dyed her hair to change her appearance. (4RT 302.)

Count 19: Identity theft of Barbara

In June 2013, Barbara received a text message from a stranger notifying her that her pictures were displayed on UGotPosted. (5RT 552.) Barbara went to the site and discovered naked photographs that she had sent to her husband; she did not know how they became posted. (5RT 553-554; ex. 33.) In the comments on the website, someone who was impersonating her was flirting with other commentators. (5RT 557.) Another commentator provided her home address, stating, “for a good time, you can find her here.” (5RT 558.) Barbara posted her own comment, pleading for someone to tell her how to remove the pictures. (5RT 557.) The website administrator allowed the comment that gave her home address to remain, but removed her plea. (5RT 559.) Barbara contacted ChangeMyReputation.com, and engaged in an online chat with someone who purported to be a woman and who offered to remove her pictures for \$5,000. (5RT 560-562.)⁹ After contacting the police, Barbara filed a DMCA notice. (5RT 563-564.) The pictures were removed, but her personal information remained. (5RT 563.) Afraid that someone would

⁹ The parties stipulated that UGotPosted.com did not interact through either a live chat or phone calls; consequently, if a website asked for \$5,000, whether by means of a phone call or live chat, it was not UGotPosted. (8RT 1046.)

stalk her, Barbara was unable to sleep at night and so installed a home security system. (5RT 560, 563.) She felt “raped” and afraid. (5RT 556-557.)

Counts 20 and 21: Identity theft and extortion of Brian

In March or April 2013, Brian began receiving unusual friend requests from strangers. (6RT 706.) When someone directed him to the UGotPosted website, he discovered his full name and town, along with links to Tumblr and his Facebook page, and both naked and clothed photos of himself had been posted without his consent. (6RT 708, 712; ex. 58.) He had taken the naked photos of himself and sent them to several people in confidence. (6RT 716, 718.) The clothed photos had been copied from his Facebook page. (6RT 717.)

Brian was embarrassed and concerned that his parents and employer would see the site. (6RT 708-709.) He contacted the website and unsuccessfully sought to have the images removed by filing a DMCA complaint. (6RT 712.) At some point, he contacted ChangeMyReputation.com and was told that if he paid \$250, the photos would be removed. (6RT 714.) Although he had reservations whether the pictures would be taken down because the web administrators for UGotPosted and ChangeMyReputation were the same, Brian paid the required sum, so that no one else would see the photos. (6RT 716-717, 721-722.) The photos were later removed. (6RT 716.)

Count 22: Identity theft of Kristina B.

Kristina was notified by a friend that she had been posted on UGotPosted.com. (4RT 339; ex. 74.) She discovered one picture of herself clothed, which had been taken from her Facebook page, and other naked photos, which she had originally sent to her boyfriend. The naked photos were intended to be private and were posted without her consent. (4RT 344.) Kristina received disgusting and vulgar messages on her Facebook

page. (4RT 341-342.) She felt embarrassed and threatened. (4RT 340-341.) She sent an email and a letter to the website, demanding that it take down the photos, but she received no reply. (4RT 344, 346.) As a result of the postings, Kristina still struggles with being able to trust anyone. (4RT 345.)

Count 23: Identity theft of Jocelyn

Jocelyn learned that pictures of her had been posted on the UGotPosted website. She discovered clothed pictures of herself, as well as pictures of body parts that purported to be hers, but were not. (4RT 309; ex. 67.) The photos were posted without her consent. (4RT 310.) The comment section listed her personal information, including the city she lived in and her cell phone number, and also included nasty and vulgar comments. (4RT 310, 316.) Some of the posters said they knew her. (4RT 311.) She received unwanted contact from strangers, and some of her co-workers also saw the website. (4RT 310, 312.) Angry, sad, threatened, and upset, she felt as if people were looking at her and judging her, even if they were not. (4RT 311-312.)

Count 24: Identity theft of Ashley

In July 2013, Ashley learned through Facebook that private photos she had sent to her boyfriend had been posted without her consent on UGotPosted.com. (4RT 330, 332; ex. 68.) Over a hundred people contacted her, harassing her sexually. (4RT 331.) Ashley contacted the website, but she never received a response. (4RT 332.) Ashley lived in a small town, and eventually the entire town came to learn of the postings. (4RT 331.) As a result, she suffered psychological, financial, and emotional trauma, and found it necessary to relocate, but even this did not help. (4RT 330-331.)

Counts 26 and 27: Identity theft and extortion of Manuel

In April 2013, Manuel began receiving Facebook messages informing him that his photos were on UGotPosted. (6RT 692.) Manuel went to the website and saw the photos, along with his Facebook link, full name, and

hometown. (6RT 698.) He had originally taken the selfies and sent them in confidence to someone he met on a dating site. (6RT 693, 700; ex. 4.) When the relationship soured, that person had threatened to post his photos if Manuel did not send additional nude photos. (6RT 700.) He tried changing his Facebook URL, but then discovered that the UGotPosted cite updated the change as well. (6RT 698.) Manuel followed a link on the website to ChangeMyReputation.com, which instructed him to take a photo of himself along with his driver's license to verify his identity, and then pay \$250 to have the photos removed. (6RT 693-695.) Manuel paid, and the photos were removed. (6RT 693.) However, even after the pictures were removed, searches on Google Images continued to return results for the website, although those results were linked to a person named "Ramon." (6RT 702.) Eventually, Manuel was successful in having Google remove the results. (6RT 703.)

The photos were "shocking" and it was upsetting to see them. (6RT 692-693.) Manuel, who is gay, had not yet come out when the photos were seen by his friends and family. (6RT 693.) He had to delete his Facebook account. After several months, he tried to go back on Facebook, but people found him because his private information was still on the Internet. (6RT 699.)

Counts 28 and 29: Identity theft and extortion of Jasmine

In June 2013, Jasmine received notice from a stranger that her photos had been posted. (5RT 583.) She went to the UGotPosted site and discovered nude pictures of herself that she had sent to a former boyfriend, as well as her full name and social media links. (5RT 583, 585; ex. 586.) A few days later, her employer, Nordstrom's, informed her that unless she had the pictures removed, she would be fired. (5RT 583-584.) Jasmine followed a link on the UGotPosted site and after paying \$249, the photos were taken down. However, the photos popped up on other sites, and Jasmine

convinced her former boyfriend, who had posted the pictures, to pay another \$249 to ChangeMyReputation.com have those images removed as well. (5RT 585, 591, 592.) The experience left Jasmine feeling frightened, embarrassed and ashamed. (5RT 586-587.)

ARGUMENT

I. APPELLANT WAS AN “INFORMATION CONTENT PROVIDER,” OR ALTERNATIVELY ACTED WITH AN INTENT TO DEFRAUD, AND THEREFORE HE WAS NOT IMMUNE TO PROSECUTION FOR IDENTITY THEFT; FURTHER, SUBSTANTIAL EVIDENCE SUPPORTS HIS CONVICTIONS

Appellant initially maintains his actions were protected under the CDA. (AOB 21.) He is mistaken. Contrary to appellant’s assertions, he did much more than simply choose which information to post—editorial functions that typically would be immune under the CDA. Instead, appellant designed the website so that posters had to provide the victims’ personal identifying information (PII). Based on the website design, appellant became responsible as a developer and provider of the content that was posted, and not merely for his editorial choices, and he thereby lost any “immunity” under the CDA. Alternatively, regardless of whether appellant was culpable for the postings themselves, he retained possession of the victims’ PII for the purpose of defrauding them into utilizing his separate website, ChangeMyReputation.com, and paying money to have their images removed.

Appellant also claims there was insufficient evidence to demonstrate that he willfully and unlawfully possessed the victims’ PII under section 530.5. (AOB 38-44.) Here, again, appellant is incorrect. Appellant required posters to include the victims’ PII and therefore he willfully received that information when the posters did what was required of them. Moreover, appellant used that information for the purpose of committing three

separate unlawful acts: violation of section 653m, intrusion into private affairs, and public disclosure of private facts.

A. Applicable Law

As with any claim of insufficient evidence, a reviewing court's role on appeal is a limited one: "In addressing a challenge to the sufficiency of the evidence supporting a conviction, the reviewing court must examine the whole record in the light most favorable to the judgment to determine whether it discloses substantial evidence that is reasonable, credible and of solid value such that a reasonable trier of fact could find the defendant guilty beyond a reasonable doubt." (*People v. Kraft* (2000) 23 Cal.4th 978, 1053-1054; *Jackson v. Virginia* (1979) 443 U.S. 307, 319.) An appellate court must presume in support of the judgment the existence of every fact the trier could reasonably deduce from the evidence. (*People v. Kraft, supra*, 23 Cal.4th at p. 1053.) The same standard applies when the conviction rests primarily on circumstantial evidence. (*People v. Snow* (2003) 30 Cal.4th 43, 66.) "Although it is the duty of the jury to acquit a defendant if it finds the circumstantial evidence susceptible of two reasonable interpretations, one of which suggests guilt and the other innocence, it is the jury, not the appellate court that must be convinced of the defendant's guilt beyond a reasonable doubt." (*Ibid.*) "If the circumstances reasonably justify the trier of fact's findings, the opinion of the reviewing court that the circumstances might also reasonably be reconciled with a contrary finding does not warrant a reversal of the judgment." (*People v. Kraft, supra*, 23 Cal.4th at p. 1054.)

Section 530.5, subdivision (a), provides in relevant part that "Every person who willfully obtains personal identifying information . . . of another person, and uses that information for any unlawful purpose" is guilty of a public offense. "Personal identifying information" is defined in section 530.55, subdivision (b), which sets forth a lengthy list of the types

of information included within the term, such as “any name, address, telephone number” as well as “date of birth, unique biometric data including fingerprint, facial scan identifiers, voiceprint, retina or iris image or other unique physical representation” and “unique electronic data including information identification number assigned to the person, address or routing code, telecommunication identifying information or access device.”

Section 530.5 includes a limited exception for certain persons or entities involved with the Internet. Namely, an “interactive computer service” or an “access software provider” as defined by the CDA are not liable unless that service or provider “acquires, transfers, sells, conveys, or retains possession of personal information with the intent to defraud.” (§ 530.5, subd. (f).)

The CDA provides tort immunity for neutral intermediaries who allow third parties to post content on their websites. (See generally *Barrett v. Rosenthal* (2006) 40 Cal.4th 33, 39-40, 62.)¹⁰ It provides: “No provider or user of an interactive computer service¹¹ shall be treated as the publisher or speaker of any information provided by another information content

¹⁰ At least one federal circuit court has questioned whether the CDA should be characterized as a defense rather than as an immunity from liability. (*Doe v. GTE Corp.* (7th Cir. 2003) 347 F.3d 655, 660; *Chicago Lawyers’ Comm. For Civil Rights Under Law, Inc. v. Craigslist, Inc.* (7th Cir. 2008) 519 F.3d 666, 670.) Respondent notes this is an open issue that need not be resolved in the present case. Respondent’s references to “immunity” should not be interpreted as suggesting that the CDA is anything more than a defense or prohibition from liability.

¹¹ The CDA defines “interactive computer service” as: “any information service, system, or access software provider that provides or enables computer access by multiple users to a computer server, including specifically a service or system that provides access to the Internet and such systems operated or services offered by libraries or educational institutions.” (47 U.S.C. § 230(f)(2).)

provider¹².” (47 U.S.C. § 230(c)(1).) This grant of immunity applies only if the interactive computer service provider is not also an “information content provider,” which is defined as someone who is “responsible, in whole or in part, for the creation or development of” the offending content. (*Id.* § 230(f)(3); *Fair Housing Council of San Fernando Valley v. Roommates.Com (“Roommate”)* (9th Cir. 2008) 521 F.3d 1157, 1162.) “[A] service provider is ‘responsible’ for the development of offensive content only if it in some way specifically encourages development of what is offensive about the content.” (*F.T.C. v. Accusearch Inc.* (10th Cir. 2009) 570 F.3d 1187, 1199.) A website operator can be both a service provider and a content provider. (*Roommate, supra*, 521 F.3d at p. 1162.) Namely, if the operator passively displays content created by third parties, then it is only a service provider with respect to that content. “But as to content that it creates itself, or is ‘responsible, in whole or in part’ for creating or developing, the website is also a content provider.” (*Ibid.*)

“The prototypical service qualifying for this statutory immunity is an online messaging board (or bulletin board) on which Internet subscribers post comments and respond to comments posted by others.” (*F.T.C. v. Accusearch, Inc., supra*, 570 F.3d at p. 1195.) The Fourth Circuit has determined that Congress’ intent in enacting the CDA was to prevent censorship of the Internet:

Congress’ purpose in providing the § 230 immunity was thus evident. Interactive computer services have millions of users. [Citation.] The amount of information communicated via interactive computer services is therefore staggering. The specter of tort liability in an area of such prolific speech would

¹² The CDA defines “information content provider” as: “any person or entity that is responsible, in whole or in part, for the creation or development of information provided through the Internet or any other interactive computer service.” (47 U.S.C. § 230(f)(3).)

have an obvious chilling effect. It would be impossible for service providers to screen each of their millions of postings for possible problems. Faced with potential liability for each message republished by their services, interactive computer service providers might choose to severely restrict the number and type of messages posted. Congress considered the weight of the speech interests implicated and chose to immunize service providers to avoid any such restrictive effect

(*Zeran v. America Online, Inc.* (4th Cir. 1997) 129 F.3d 327, 331

Nonetheless, in enacting these protections Congress was equally clear that it intended “to ensure vigorous enforcement of Federal criminal laws to deter and punish trafficking in obscenity, stalking, and harassment by means of computer.” (47 U.S.C. § 230(b)(5).) To effectuate this policy, the CDA specifically provides that nothing in that Act is intended to impair the enforcement of any federal criminal statute (47 U.S.C. § 230(d)(1)), and likewise nothing in the Act “shall be construed to prevent any State from enforcing any State law that is consistent with [that] section.” (47 U.S.C. § 230(d)(3)).

Thus, the CDA does not protect those who intentionally commit crimes on the Internet. “When Congress passed section 230 it didn’t intend to prevent the enforcement of all laws online; rather, it sought to encourage interactive computer services that provide users *neutral* tools to post content online to police that content without fear that through their ‘good samaritan [sic]. . . screening of offensive material,’ 47 U.S.C. § 230(c), they would become liable for every single message posted by third parties on their website.” (*Roommate, supra*, 521 F.3d at p. 1175 [emphasis in original].) If a website operator’s conduct is “unlawful when [conducted] face-to-face or by telephone, [it doesn’t] magically become lawful when [conducted] electronically online.” (*Id.* at p. 1164.)

Appellant does not fall within the exception under section 530.5, subdivision (f), both because he was an “information content provider” as

to the relevant content, and, in any event, he retained possession of the victims' personal information with the intent to defraud.

B. Appellant Was an Information Content Provider and Therefore Fell Outside the Exclusion of Penal Code Section 530.5, Subdivision (f)

Appellant is not entitled to immunity under the CDA because he went well beyond the role of a mere editor. He was responsible for the content of the site by virtue of his design of the site's required fields, which made users post the victims' private information as a condition of use.

Appellant briefly mentions the Ninth Circuit's decision in *Roommate* (AOB 29), but does not otherwise discuss that decision, even though it featured prominently in the court below. In *Roommate*, the Ninth Circuit held that the CDA did not immunize a website when it engaged in unlawful housing discrimination. (*Roommate, supra*, 521 F.3d at p. 1175.) There, the website "Roommates.com" was designed to match people renting out spare rooms with those looking to rent. (*Id.* at p. 1161.) As conditions of use, the website required subscribers to disclose their sex, sexual orientation, and whether they would bring children to the household, and also required subscribers to select their preferences with respect to the same three criteria. (*Ibid.*) The Fair Housing Councils of San Fernando Valley and San Diego sued the website for violating federal and state housing discrimination laws. The Ninth Circuit, sitting en banc, rejected Roommate's assertion that it was protected by the CDA, holding: "The CDA does not grant immunity for inducing third parties to express illegal preferences. Roommate's own acts—posting the questionnaire and requiring answers to it—are entirely its doing and thus section 230 of the CDA does not apply to them. Roommate is entitled to no immunity." (*Id.* at p. 1165.) As the Ninth Circuit reasoned, "Here, the part of the profile that is alleged to offend the Fair Housing Act and state housing discrimination

laws—the information about sex, family status and sexual orientation—is provided by subscribers in response to Roommate’s questions, which they cannot refuse to answer if they want to use defendant’s services.” (*Id.* at p. 1166.) More succinctly, “Unlawful questions solicit (a.k.a. ‘develop’) unlawful answers.” (*Ibid.*)

In addressing the separate question of whether Roommate was entitled to immunity for its search engine, which allowed users to search by the same discriminatory factors, the Ninth Circuit proposed a “material contribution” test to determine whether a person is responsible “in whole or in part” (47 U.S.C. § 230(f)(3)) as a developer of the illegal content. (*Id.* at p. 1168.) By way of example, the court observed that a dating website that required users to provide their sex, race, religion and marital status, and allowed searches based on those responses, would not constitute a material contribution to any alleged illegality because there is nothing illegal with discriminating along these lines in the context of dating. (*Id.* at p. 1169 & fn. 23.) Applying these principles, the court concluded that Roommate’s connection to the discriminatory filtering process was “direct and palpable.” (*Id.* at p. 1169.) Based on the design of the website, the Ninth Circuit distinguished cases in which an editor simply decides whether to exclude material that a third party seeks to post, or a website simply provides a forum where others choose to post illegal content. (*Id.* at pp. 1170-1171 [distinguishing *Batzel v. Smith* (9th Cir. 2003) 333 F.3d 1018, and *Carafano v. Metroplach.com, Inc.* (9th Cir. 2003) 339 F.3d 1119].) In contrast to these situations, Roommate both elicited the allegedly illegal content and made “aggressive use of it” in conducting its business. (*Id.* at p. 1172.)

While holding Roommate liable for the required fields and website design, the Ninth Circuit reached a different conclusion regarding an open comments section in which users were able to enter additional remarks

regarding the type of roommate they were seeking. Although some of these additional comments expressed discriminatory preferences, the mere fact that Roommate encouraged users to provide “something” was not enough to render it a developer of content: “. . . Roommate does not tell subscribers what kind of information they should or must include as ‘Additional Comments,’ and certainly does not encourage or enhance any discriminatory content created by users.” (*Id.* at p. 1174.) Such a “generic text prompt,” as would commonly occur with a typical search engine, would be immune from liability where there is “no direct encouragement to perform illegal searches or to publish illegal content.” (*Id.* at p. 1175.)

Here, similar to the situation in *Roommate*, appellant willfully obtained individuals’ personal identifying information by soliciting it from submitters, who were required to include the victims’ full name, location (“city, state, country”), age, and a link to the victims’ Facebook profile page in order to submit photographs. As in *Roommate*, appellant became responsible for the illegal content of the postings because the illegal content (i.e., the non-consensual use of someone’s personal identifying information, including their private photos) was a condition of use. Appellant then used that information to harass and annoy victims because he knew—with absolute certainty—that by posting the information, the victims would be contacted by numerous strangers whom the victims would find threatening. Appellant also used the information for the unlawful purpose of unlawfully obtaining money from them by demanding payment in exchange for removing his posts. This conduct does not magically become lawful because appellant did it online, or because he recruited third parties to help him inflict harm on a mass scale.

Rather than address *Roommate*, appellant instead discusses cases holding that a service provider is not liable for the exercise of a publisher’s traditional editorial functions, such as deciding whether to publish or edit

content. (AOB 30; see *Barnes v. Yahoo! Inc.* (9th Cir. 2009) 570 F.3d 1096, 1102; *Carafano v. Metrosplash.com, Inc.*, *supra*, 339 F.3d 1119; *Batzel v. Smith*, *supra*, 333 F.3d 1018; *Zeron v. America Online, Inc.*, *supra*, 129 F.3d 327.) But this argument is nothing more than a strawman. Appellant is culpable, and he is not immune under the CDA, because his website design required the unlawful content, not because he exercised editorial discretion.¹³ Appellant’s suggestion that he simply asked for “statistical information” with which there is nothing “inherently wrong” (AOB 33-34) is palpably incorrect. First, this case does not involve mere “statistical information.” In order to submit photographs, a submitter had to include the victim’s first and last name, location (including city, state, and country), age, and a link to the victim’s Facebook page. These were all required fields, as were the photos themselves (5RT 452-454), and they fell squarely within the definition of PII under section 530.55, subdivision (b). Second, the information was obtained for an unlawful purpose, as the jury necessarily found. As *Roommate* underscored, the present case is not like a dating website, in which it is permissible to request information regarding a user’s sex or sexual orientation, because there is nothing illegal with such information in that context. Here, as discussed further below, appellant obtained the information for the unlawful purposes of invading the victims’ rights of privacy, committing extortion, and violating section 653m. (Cf. *Doe II v. MySpace Inc.* (2009) 175 Cal.App.4th 561, 575 [distinguishing

¹³ To be sure, appellant’s editorial choices provided useful evidence of his scheme and intent, but they are not the reason that he fell outside of the CDA’s immunity. Nor is it sufficient that appellant was on notice of the unlawful nature of the information posted on his website (*Universal Communication Systems, Inc. v. Lycos, Inc.* (1st Cir. 2007) 478 F.3d 413, 420), although here again the nature of that information is relevant to demonstrating appellant’s purpose and motive.

Roommate, court noted there was no allegation that MySpace’s profile questions are “discriminatory or otherwise illegal”].)

Unlike the cases on which he relies (AOB 30-33), appellant did not simply operate an otherwise content-neutral search engine or online bulletin board, which a third party used to publish disparaging or defamatory material. In such cases, an operator’s ability to edit or screen postings is insufficient to render the defendant civilly liable. Here, in contrast, appellant was responsible for the content that his website required users to provide, not merely his editing choices.

For similar reasons, appellant’s reliance (AOB 34-35) on *Jones v. Dirty World Entertainment Recordings, LLC* (6th Cir. 2014) 755 F.3d 398 (“*Dirty World*”) is also misplaced. There, defendant Nik Richie operated a website, TheDirty.com, which relied on anonymous third parties to supply “dirt” or gossip on any subject. The website staff would review the submissions and choose which were appropriate for publication, and the defendant would typically add a short one-line humorous comment. (*Id.* at p. 403.) The website ran a series of submissions impugning the sexual reputation of a professional cheerleader, who sued Richie as operator of the site for defamation. (*Id.* at p. 401.) Based on these facts, the Sixth Circuit held that Richie and the website had immunity under the CDA because he did not materially contribute to the creation or development of the offending material and, therefore, was not an information content provider. (*Id.* at pp. 415-416.) In reaching this holding, the court distinguished the Ninth Circuit’s *Roommate* decision on the grounds, inter alia, that the website there required subscribers to disclose illegal or actionable content about “protected characteristics” as a condition of use. (*Id.* at pp. 411, 416.) The Sixth Circuit further pointed out that the name of the website, “TheDirty.com,” did not suggest that only illegal or actionable content would be published. (*Id.* at p. 416.) Finally, although Richie acted as an

information content provider when he added his absurd, one-line comments, those comments did not materially contribute to the defamatory content of the challenged postings. (*Ibid.*)

The present case is like *Roommate* and unlike *Dirty World*. Appellant's extortion scheme would not have worked without the victims' personal identifying information. In order not to be just another online pornography site with photos of anonymous people, appellant had to link the photos to specific individuals who could then be contacted. Hence, unlike *Dirty World*, appellant's website required users to post illegal or actionable content as a condition of use. Appellant's own acts in designing the site to require submitters to provide not only graphic photographs, but also other personal identifying information, and then posting that information with intent to cause harm to victims and extort them, place him outside the scope of CDA's immunity provisions. As the name of the website "UGotPosted.com" itself revealed, it was intended to notify victims that someone else had posted their private information online. (Cf. *Dirty World, supra*, 755 F.3d at p. 416 ["Nor does the name of the website, www.TheDirty.com, suggest that only illegal or actionable content will be published"].) Appellant knew the information was furnished without the victims' consent because the very purpose of his website was to shame victims into paying him money. As in *Roommate*, appellant's creation and design of the website registration process made him an information content provider as to the answers he solicited. He knowingly sought to transform virtually unknown information—the victims' graphic photographs and personal identifying information—into a commodity which he could use to extort victims. (Cf. *F.T.C. v. Accusearch Inc., supra*, 570 F.3d at p. 1199 [In denying CDA immunity, court held, "Accusearch solicited requests for such confidential information and then paid researchers to obtain it. It knowingly sought to transform virtually unknown information into a

publicly available commodity. And as the district court found and the record shows, Accusearch knew that its researchers were obtaining the information through fraud or other illegality”]

In the court below, appellant attempted to distinguish Roommate on the basis that the website there was designed to require users to select from pre-populated answers, whereas appellant’s website required posters to input original information. (7RT 944.) Appellant apparently no longer pursues that argument here, and properly so. Whether a poster uses a pull down menu or provides his own data, the results are the same in a case such as this where the poster was required to provide illegal content consisting of the victims’ PII and private photos. Appellant cites *Carafano v. Metroplash.com, Inc., supra*, 339 F.3d 1119, where the Ninth Circuit held that a computer matchmaking service was immune under the CDA when an unknown person created a false dating profile for a well-known actress. Although some of the content in the profile was based on responses to the site’s questionnaire, which included multiple choice answers, the Ninth Circuit concluded that “the selection of the content was left exclusively to the user,” and therefore the site could not be considered an information content provider. (*Id.* at p. 1124.) But the dating website in *Carafano* did not require users to provide illegal content; indeed, most of the customers presumably provided legitimate information in the hope of meeting a match. In Roommate, the Ninth Circuit specifically distinguished *Carafano* on this basis:

By contrast, Roommate both elicits the allegedly illegal content and makes aggressive use of it in conducting its business. Roommate does not merely provide a framework that could be utilized for proper or improper purposes; rather, Roommate’s work in developing the discriminatory questions, discriminatory answers and discriminatory search mechanism is directly related to the alleged illegality of the site

(*Roommate*, 521 F.3d at p. 1172.) The same is equally true of appellant's site.

The only purpose of appellant's website was to harass, annoy, extort, and otherwise harm victims. Appellant did not maintain a neutral bulletin board that merely refrained from removing offensive content. Rather, he only allowed content that harmed victims by disclosing their personal identifying information along with their private graphic photographs. Consequently, because he was responsible for developing the content of the site, he was an information content provider and he was not immune from prosecution under the CDA.

C. Appellant Retained Possession of Personal Identifying Information with the Intent to Defraud the Victims

Alternatively, even if appellant were not an information content provider, he did not fall within the exception of section 530.5, subdivision (f), because he retained the victims' personal identifying information with the intent to defraud. Specifically, appellant operated the ChangeMyReputation.com website with the intent to deceive victims into believing that it was separate from the UGotPosted.com site on which their pictures were posted.

“ ‘ “Intent to defraud is an intent to commit a fraud.” [Citation.] ‘ “Fraud” ’ and ‘ dishonesty ’ are closely synonymous. Fraud is defined as ‘ a dishonest stratagem. ’ [Citation .] It ‘ may consist in the misrepresentation or the concealment of material facts ’ [citation], or a statement of fact made with ‘ conscious[ness] of [its] falsity. ’ [Citation.] ” [Citation.] ” (*People v. Booth* (1996) 48 Cal.App.4th 1247, 1253.)

Here, the evidence amply demonstrated appellant's intent to defraud. When victims asked to have the offending photos removed, they were either referred to the website “ChangeMyReputation.com,” or they followed the link to that site. (E.g., 5RT 600.) This extra step was wholly

unnecessary. Appellant could have removed the photos by demanding the money directly from the victims as part of the UGotPosted website. But appellant presumably realized that the victims would be less inclined to pay money to the very person responsible for posting their pictures. By creating a separate website, appellant hoped to deceive the victims into believing that they were receiving the legitimate services of a neutral third party who would restore their reputation, and that they were not simply paying blackmail to an extortionist who was the source of their misery.

Appellant maintains that he made no attempt to hide the fact that the sites were related, and points out that he included a link to the ChangeMyReputation.com site on the UGotPosted webpage, and also that the connection between the sites was obvious to some of the victims. (AOB 27.) But intent to defraud does not require actual reliance by the person intended to be defrauded as in the case of a completed fraud. (*People v. Reed* (1961) 190 Cal.App.2d 344, 353.) Victims repeatedly testified that they received no response when they contacted the UGotPosted website directly (e.g., 4RT 272, 276, 354, 356; 5RT 404); appellant would, however, respond to inquires sent to ChangeMyReputation.com. (e.g., 5RT 599-600; 6RT 633-636). A reasonable jury could well conclude that appellant went to the effort to distinguish these two websites in order to portray the fees charged on ChangeMyReputation.com as a legitimate reputation cleansing service. Although appellant may have found it useful to link that website so that victims would be able to find it, it does not mean he did not intend to defraud them into believing the site belonged to a separate business. In the same way that appellant represented himself as “James Smith” to one victim (4RT 324-325), he also endeavored to conceal the true identities of his businesses. Whether his intent was successful is a wholly separate matter; section 530.5, subdivision (f), does not require that anyone actually be defrauded.

D. There Was No First Amendment Violation

Although appellant at times references the First Amendment (e.g., AOB 38), he cites neither authority nor reason to suggest a constitutional violation in the present case. Accordingly, he has not properly presented any such issue for appeal. (See, e.g., *People v. Gionis* (1995) 9 Cal.4th 1196, 1214, fn. 11 [matters perfunctorily asserted without argument or authorities in support not properly raised on appeal].)

In any event, there was no violation of the First Amendment. As the United States Supreme Court has long observed, “it has never been deemed an abridgement of freedom of speech or press to make a course of conduct illegal merely because the conduct was in part initiated, evidenced, or carried out by means of language, either spoken, written, or printed.” (*Giboney v. Empire Storage & Ice Co.* (1949) 336 U.S. 490, 502.) “Extortion is not a constitutionally protected form of speech.” (*Flatley v. Mauro* (2006) 39 Cal.4th 299, 328; see also *R.A.V. v. City of St. Paul* (1992) 505 U.S. 377, 420 (conc. opn. of Stevens, J.) [“Although the First Amendment broadly protects ‘speech,’ it does not protect the right to ... ‘extort’ ”]; *United States v. Quinn* (5th Cir. 1975) 514 F.2d 1250, 1268 [“It may categorically be stated that extortionate speech has no more constitutional protection than that uttered by a robber while ordering his victim to hand over the money, which is no protection at all”].) To the extent that appellant has preserved a First Amendment challenge, he has not shown a violation of the Constitution.

E. Appellant Willfully Obtained Personal Identifying Information

Appellant maintains there was insufficient evidence that he willfully obtained the victims’ personal identifying information. (AOB 38-39.) His claim is meritless. Section 530.5, subdivision (a), requires, among other things, that the defendant “willfully” obtained someone else’s personal

identifying information. (2CT 381; CALCRIM No. 2040.) “The word ‘willfully,’ when applied to the intent with which an act is done or omitted, implies simply a purpose or willingness to commit the act, or make the omission referred to. It does not require any intent to violate law, or to injure another, or to acquire any advantage.” (§ 7, subd. (1).) Here, appellant specifically solicited personal identifying information on his website; he therefore willfully received it when third parties answered his call and submitted the information to be posted. Appellant’s point that he received the information from third parties and not the owner of the information (AOB 39-40) is immaterial. There is no requirement under section 530.5 that a defendant receive the information directly from the owner, rather than from an intermediary. Nor would any such requirement make any sense; it would simply encourage criminals such as appellant to launder personal identifying information through shells and shell entities in order to avoid liability.

F. Appellant Used the Personal Identifying Information for an Unlawful Purpose

Appellant also maintains there was insufficient evidence that he used the PII for an unlawful purpose. (AOB 41-44.) Contrary to his argument, there was ample evidence that appellant committed three separate unlawful acts: violation of section 653m, intrusion into private affairs, and public disclosure of private facts. Even if there were insufficient evidence to support one of these three theories, the convictions may stand based on the other two.

1. Section 653m

An unlawful purpose, under section 530.5, subdivision (a), includes facilitating the crime of contact by electronic communication device with intent to annoy or harass under section 653m, subdivision (a). (*In re Rolando S.* (2011) 197 Cal.App.4th 936, 947 [holding that harassing and

annoying under section 653m, subd. (a), constitutes an unlawful purpose].)

Section 653m, subdivision (a), provides:

Every person who, with intent to annoy, telephones or makes contact by means of an electronic communication device with another and addresses to or about the other person any obscene language or addresses to the other person any threat to inflict injury to the person or property of the person addressed or any member of his or her family, is guilty of a misdemeanor. Nothing in this subdivision shall apply to telephone calls or electronic contacts made in good faith.

Appellant contends that this provision does not apply to him because there was no evidence that he personally made contact with any of the victims. (AOB 42.) But the language of the 653m is very precise: it does not say that the defendant must personally contact the victim. That language provides that the defendant either “telephones or *makes contact* by means of an electronic communication device with another.” (Italics added.) The verb “telephones” arguably requires action by the defendant himself. But “makes contact” is deliberately more vague. It is possible to make contact without directly contacting the victim, for instance by use of a third party. Had the Legislature intended to require that the defendant personally and directly “contact” the victim, it would not have inserted the word “makes” and would simply have used the word “contacts.” Here, appellant made contact by relying on the posters and other persons viewing the site to notify the victims. Notably, all the victims in the charged counts were made aware of the postings, as appellant knew they would be.

Appellant required the posters to include the victims’ names, ages, addresses, and social media information so that they would be immediately contacted and harassed. The postings actually included the links, i.e., the victim’s “unique electronic data,” that would take a viewer of the website directly to the victim’s social media address so that they could easily harass the victim. There is no question the victims were indeed harassed. If not,

the scheme would not have worked. The unsolicited contacts terrified the victims. They received hundreds of unwanted disparaging and vulgar contacts, some even threatening rape. Thus, appellant “ma[d]e[] contact” with the victims. It is irrelevant he did not personally contact them; indeed, the use of third parties increased the harassment of and threats to the victims.

Moreover, the evidence suggested that appellant did personally contact many of the victims. When victims inevitably reached out to ChangeMyReputation.com, appellant would typically return the contact and inform them how much they would have to pay. (E.g., 4RT 283; 5RT 404, 600, 602; 6RT 633-636, 714.) Other times appellant would respond that the victims needed to provide additional pictures or identification. (E.g., 4RT 325; 6RT 693-695.) That these contacts may have been in response to initial inquiries by the victims is immaterial; under the language of the statute, appellant still “ma[d]e[] contact.”

Finally, as discussed in greater detail below in the context of the extortion counts (see Argument II, *infra*), the intent behind these contacts, and indeed behind the website itself, was to convey the threat that unless the victims paid money, their PII and photos would remain posted. Accordingly, there was substantial evidence of a threat to inflict injury to the person or property.

2. Intrusion into private affairs

An unlawful purpose may also be based on the commission of an intentional tort. (*In re Rolando S.*, *supra*, 197 Cal.App.4th at p. 946.) Appellant maintains there was insufficient evidence he committed the tort of intrusion into private affairs, both because the photos were submitted by third parties and because the victims lacked reasonable expectations of privacy. (AOB 42-44.) Both assertions lack merit.

The common law tort of intrusion into private affairs requires an intentional intrusion into the private affairs of another in a manner that would be highly offensive to a reasonable person. (5 Witkin Summary of California Law, Torts, § 658 p. 963; 2CT 387 [CACI 1800].) The victim must have “an objectively reasonable expectation of seclusion or solitude in the place, conversation or data source.” (*Shulman v. Group W Productions, Inc.* (1998) 18 Cal.4th 200, 232.)

Without elaboration, appellant suggests that he did not commit the tort because he did not know any of the victims and instead third parties sought out his website in order to post the photos “on their own free will.” He maintains that he could not even tell “from the submissions” whether the posters were submitting photos of themselves, or someone else. (AOB 43.) But the mere fact that appellant relied on other persons to provide the photos and PII does not somehow absolve him of responsibility. He still publicly intruded into the private affairs of another even if he worked in tandem with others and even if the person who submitted the photos was authorized to see or possess them at one time. (*Shulman v. Group W Productions, Inc.*, supra, 18 Cal.4th at p. 232 [“To prove actionable intrusion, the plaintiff must show the defendant penetrated some zone of physical or sensory privacy surrounding, *or obtained unwanted access to data about, the plaintiff*”] (italics added).)

Further, his assertion that he did not know whether the posters were the persons depicted in the photos is demonstrably incorrect. The site was designed to require both the email of the submitter and the full name of the person posted. (5RT 452-453.) On over 2,300 occasions, appellant used the submitted links to Facebook to compare those photos to the photos of the people posted in order to verify their identities. (5RT 493-494.) Appellant acknowledged to Special Agent Nichol that the site was generally used by people trying to ridicule others, but he also recognized knowing that some

posters submitted pictures of themselves because they were exhibitionists. (2CT 302.) Clearly, appellant made it his business to know exactly who it was who “got posted.”

Next, appellant maintains that the victims did not have a reasonable expectation of privacy in the photos because “most” of the victims knowingly allowed the photos to be taken, and they shared them with others. (AOB 43.) Of course, not all of the victims willingly took the photos. Some of the victims were drugged or had the photos taken without their knowledge; others willingly took the photos of themselves, but had the photos stolen; and others had been photo-shopped. (See, e.g., 4RT 277-281, 309; 5RT 544, 546; 6RT 648, 771.) More importantly, even as to those victims who knowingly and willingly took “selfies,” the mere act of sharing those photos with others did not extinguish all reasonable expectations of privacy. Namely, a victim need not have an expectation of complete privacy in order to state a cause of action for intrusion into private affairs. (*Sanders v. American Broadcasting Cos.* (1999) 20 Cal.4th 907, 915 (*Sanders*)). In *Sanders*, for instance, an undercover television reporter obtained employment as a “telepsychic” and covertly videotaped conversations among co-workers. Although the co-workers recognized that their conversations might be overheard by other employees in their cubicles, they did not anticipate that their discussions would be broadcast on television for the world to hear. The court held that, “where the other elements of the intrusion tort are proven, the cause of action is not defeated as a matter of law simply because the events or conversations upon which the defendant allegedly intruded were not completely private from all other eyes and ears.” (*Id.* at p. 911.) “Privacy for purposes of the intrusion tort must be evaluated with respect to the identity of the alleged intruder and the nature of the intrusion.” (*Id.* at p. 918; see also p. 920 [“the reasonableness of a person’s expectation of visual and aural privacy depends not only on

who might have been able to observe the subject interaction, but on the identity of the claimed intruder and the means of intrusion”].) Consequently, a victim may have a legitimate expectation in limited privacy; the court eschewed the notion that an expectation of privacy “is nonexistent if not complete.” (*Id.* at p. 919; cf. *Dietemann v. Time, Inc.* (9th Cir. 1971) 449 F.2d 245, 249 [“One who invites another to his home or office takes a risk that the visitor may not be what he seems, and that the visitor may repeat all he hears and observes when he leaves. But he does not and should not be required to take the risk that what is heard and seen will be transmitted by photograph or recording, or in our modern world, in full living color and hi-fi to the public at large or to any segment of it that the visitor may select”].)

As *Sanders* instructs, simply because a victim exchanges photographs with a limited number of people, it does not follow that the victim does not retain a reasonable expectation of privacy that the photographs will not be distributed to the world at large. Appellant does not discuss *Sanders*, and instead cites two federal decisions for the general proposition that “transmissions over the Internet are not reasonably expected to be private.” (AOB 43-44, citing *United States v. Lifshitz* (2d Cir. 2004) 369 F.3d 173 and *Four Navy SEALs v. Associated Press* (S.D. Cal. 2005) 413 F.Supp.2d 1136, 1143.) Neither of those cases supports the surprising proposition that a person loses all expectations of privacy in a communication by sending it over the Internet. *Lifshitz* arose in the decidedly distinct context of the expectations of privacy of convicted sex offenders when their computers are monitored by the government as a condition of probation, and it discussed transmissions intended for publication or public posting. (*United States v. Lifshitz, supra*, 369 F.3d at p. 190.)

In *Four Navy SEALs*, on the other hand, the plaintiffs were “active duty military members conducting wartime operations in full uniform who

chose to allow their activities to be photographed and placed on the Internet.” (*Four Navy SEALs v. Associated Press, supra*, 413 F.Supp.2d at p. 1143.) A reporter discovered the photographs on an Internet website and republished them in connection with a story regarding abuses by the military during the Iraq war. Under these facts, the court held that the plaintiffs could not state a claim for invasion of the state constitutional right to privacy. (*Ibid.*) This holding makes sense, because the SEALs did not have an expectation of privacy at the time the photos were taken of them while dressed in full uniform and conducting military operations, and therefore they did not have an expectation of privacy when those photos were later posted on-line. Obviously, those facts are not present here. Here, the victims may have consented (in some instances) to have their private photos shared with specific individuals, but like the private conversations in *Sanders*, they did not anticipate that those photos would then be published worldwide. Further, information collection techniques may well be socially acceptable when conducted by a journalist in pursuit of a socially or politically important story (such a story about military abuses during war), but highly offensive “when done for socially unprotected reasons—for purposes of harassment, blackmail or prurient curiosity for example.” (*Shulman v. Group W Productions, Inc., supra*, 18 Cal.4th at p. 237.) Appellant’s actions fall squarely within the latter examples.

3. Public disclosure of private facts

Finally, appellant does not mention the separate unlawful tort of public disclosure of private facts, and thus he apparently does not contest that there was sufficient evidence that he committed that unlawful tort. (See AOB 42-43.) This tort requires a public disclosure of a private fact that is objectionable to a reasonable person and that is not of legitimate public concern. (Witkin, *supra*, at p. 974, citing *Diaz v. Oakland Tribune* (1983) 139 Cal.App.3d 118, 126; 2CT 388 [CACI 1801].) Here, any

reasonable person would object to the private facts disclosed on the website. Moreover, these facts were not the subject of legitimate public concern. (See generally *Melvin v. Reid* (1931) 112 Cal.App. 285 [cause of action stated where the defendant made a film that he advertised as the true story of the named plaintiff, and the plaintiff sued on the grounds that she had given up her former life and that the film had subjected her to ridicule])

4. Any error was harmless

Even if there were insufficient evidence to support any one of the three separate theories of unlawful conduct, any error was harmless. First, as to renumbered counts 2, 4-6, 8-15, 19, 23, and 26 the jury returned special findings that appellant committed public disclosure of private facts. As noted above, appellant does not contest that theory. Second, even as to the counts in which the jury did not unanimously agree as to at least one theory (i.e., counts 7, 17, 20, 22, 24, and 28), affirmance is required because the “jurors’ ‘own intelligence and expertise’” would have saved them from relying on any factually inadequate theory. (*People v. Guiton* (1993) 4 Cal.4th 1116, 1131.)

II. SUBSTANTIAL EVIDENCE SUPPORTS APPELLANT’S CONVICTIONS FOR EXTORTION

Appellant asserts there was insufficient evidence to support the extortion convictions because once the photos and PII were placed on the Internet for all to see, the cat was out of the bag and the victims no longer had a secret that could be disclosed. (AOB 51.) Alternatively, he maintains that he was under no obligation to remove the postings from his site and contends he therefore cannot be convicted of extortion because he was simply offering a “service” and engaging in “standard business practice.” (AOB 45.) This case, however, is not about incidental harms caused by a free market economy run amok. Appellant is a criminal who intentionally

harmed thousands of people, not a legitimate businessman. While many people knew the victims' secrets (only because appellant had exposed them on his website), many others had not yet seen the photos and it was that threat of continued exposure that appellant used to extort money from the victims. Further, because the website contained the victims' PII, and because appellant's website required posters to provide that PII, appellant was obligated to remove the content and he was not simply providing a service that he otherwise had a legal right to perform.

Extortion is the "obtaining of property from another, with his consent, or the obtaining of an official act of a public officer, induced by a wrongful use of force or fear, or under color of official right." (§ 518.) As relevant to the present case,¹⁴ the fear used to commit extortion may be based on a threat to do either of the following:

3. To expose, or to impute to him or them a deformity, disgrace, or crime; or,
4. To expose any secret affecting him or them.

(§ 519)¹⁵

As courts have frequently summarized, it is not necessary that a secret be wholly unknown to all people in order for a victim to be extorted:

"The 'secret' referred to in the statute is a matter 'unknown to the general public, *or to some particular part thereof which might be interested in obtaining knowledge of the secret*; the secret must concern some matter of fact, relating to things past, present or future; the secret must affect the threatened person in some way so far unfavorable to the reputation or to some other

¹⁴ These were the only two theories on which the jury was instructed. (2CT 379.)

¹⁵ Section 519 has been twice amended since Appellant committed his offenses in 2013. (See Stats. 2013, ch. 572, §1, and Stats. 2014, Ch. 71, §123.) Among other changes, the current version has replaced the word "any" with "a" in subdivision (4).

interest of the threatened person, that threatened exposure thereof would be likely to induce him through fear to pay out money or property for the purpose of avoiding the exposure.’ [Citation].”

(*Cross v. Cooper* (2011) 197 Cal.App.4th 357, 387, italics added.)

Whether conduct constitutes a threat must be determined under the totality of the surrounding circumstances. “No precise words are necessary to convey a threat. Conduct takes its legal color and quality more or less from the circumstances surrounding it.” (*People v. Massengale* (1968) 261 Cal.App.2d 758, 765.) “Threats may consist of a menace of destruction or injury to person or property. No precise or particular form of words is necessary in order to constitute a threat under the circumstances. Threats can be made by innuendo and the circumstances under which the threat is uttered and the relations between [complainants and defendants] may be taken into consideration in making a determination of the question involved.” (*Ibid.*; see also *People v. Oppenheimer* (1962) 209 Cal.App.2d 413, 422 [evidence that defendants entered the victim’s property and proceeded to cut trees over the victim’s objections in a menacing and bullying fashion and then demanded payment for the bill “clearly establishe[d] the crime of extortion”]; *People v. Choynski* (1892) 95 Cal. 640, 642 [extortionists “seldom possess the hardihood to speak out boldly and plainly, but deal in mysterious and ambiguous phrases. . . .”].) “Whether a threatened exposure would have this effect on the victim is a factual question and depends on the nature of the threat and the susceptibility of the victim. [Citations.]” (*Cross v. Cooper, supra*, 197 Cal.App.4th at p. 387.)

A defendant need not use threatening language in order to convey a threat. “An experienced extortionist does not find it necessary to designate specifically what he intends to do as a means of terrorizing his prey. The more vague and general his actions and statements the better they will serve

his purpose in magnifying the fear of his victim and the better also it will serve to protect him in the event of the failure to accomplish his extortion and of a prosecution of his attempted crime.” (*Massengale, supra*, 261 Cal.App.2d at pp. 764-765.) Courts have recognized that “[h]uman ingenuity being what it is, there might very well be a variety of expressions which an ingenious mind could create to convey threats without using any definite phraseology. Yet such language might under certain circumstances be sufficient to impress the mind of the person threatened as to accomplish the end in view.” (*Oppenheimer, supra*, 209 Cal.App.2d at p. 424 [discussing threats in the context of section 523, “Threatening Letters,” which references section 519, defining “threats”].)

Here, appellant induced fear by threat to expose a secret (§ 519, subd. (4)) because he posted the victims’ private photographs and accompanying personal identifying information, and he implicitly threatened to keep posting those graphic images online until the victims paid. Alternatively, appellant also exposed or imputed to the victims a disgrace (§ 519, subd. (3)) in that the pictures are graphic, private, and falsely imply the victims are wanton, licentious, or lustful. (See, e.g., *Leser v. Penido* (2009) 879 N.Y.S.2d 107, 108 [naked pictures connected to victim’s name and photograph on various websites falsely implied that she is sexually lustful and promiscuous]; *Rejent v. Liberation Publications, Inc.* (1994) 611 N.Y.S.2d 866, 867 [cause of action for defamation stated where sexually suggestive photos falsely implied plaintiff was lustful and promiscuous].)

Contrary to appellant’s assertions (AOB 51), under the totality of the circumstances he clearly conveyed a threat to the victims. In posting the personal identifying information of the victims, appellant knew—with absolute certainty—that the victims would be contacted by dozens, if not hundreds, of strangers trolling the Internet. Any reasonable person would find this contact, which often included a link to the site “UGotPosted,”

frightening and would naturally and predictably visit the website. Appellant knew that when the victims inevitably contacted his website, they would see the name of the site prominently displayed: UGotPosted.com. They would see graphic and explicit photographs of themselves. What was worse, these were not simply anonymous pictures. Because the victims' names, Facebook addresses, and other identifying information were required fields for every posted entry, the victims would discover that these most intimate photographs were specifically identified as depicting them. They also would see the frequently threatening and humiliating comments posted by persons who had already viewed the pictures. Victims testified that when they viewed their UGotPosted profile pages, they would find appellant's contact email or a link to his website "ChangeMyReputation." When contacted, appellant often directed them to ChangeMyReputation or instructed them to pay. As appellant intended, his message was conveyed. The threat was obvious, essentially: "pay me or I will continue to humiliate you and subject you to infinite harm."

Significantly, appellant was able to convey a threat of harm that was boundless. Among many other harms, the continuing publication of the shaming profiles subjected the victims to ongoing threats of community humiliation and ongoing threats of physical attack by the goblins of the Internet who now had their most private information and knew how to reach them. Any person would find appellant's conduct threatening, and any person in appellant's position would know that he was conveying a threat of substantial harm to the victims.

Appellant asserts that there could not be a threat to expose a secret because once the photos and identifying information were posted on the Internet, they were "already in the public domain" and could no longer be considered secrets. (AOB 47.) He insists that all he did was provide a means to remove these non-secrets for a fee. (AOB 48.)

Appellant is mistaken for several reasons. First, a secret must be unknown to the general public or some particular part thereof. (*People v. Lavine* (1931) 115 Cal.App. 289, 295 (*Lavine*)). A secret does not cease to be a secret simply because it is known by others, or even a large number of people, as long as there are some people who do not know it. (*People v. Peniston* (1966) 242 Cal.App.2d 719, 723 (*Peniston*)).

The decision in *Peniston* is instructive. There, the Court of Appeal held that a threat to expose nude photographs of the victim to her husband and parents constituted sufficient evidence of extortion even though those same photographs were widely circulated throughout the Pacific Coast. (*Peniston, supra*, 242 Cal.App.2d at p. 722.) Specifically rejecting an additional evidentiary claim that the court improperly excluded motion pictures of the victim, which were widely exhibited in arcades in the San Fernando Valley and which would have shown that the pictures were not a secret to the general public, the *Peniston* court concluded, “We think the trial judge correctly focused on the true issues in the case, whether [the victim’s] husband and parents knew about the pictures and whether the threat of disclosure to them put [the victim] in fear.” (*Id.* at p. 723.)

Here, the victims’ private disclosure of the photos to one or two people did not mean the pictures were no longer a secret, nor did the fact that many, perhaps even millions of people on the Internet, had already seen them, prevent the photos from being a secret as to the millions of others who had not. Even once the pictures were displayed on the Internet, the continued exposure threatened disclosure to people who had not yet seen them. The mere fact that many people had seen the pictures already did not detract from the continuing nature of the threat; many more people had not seen the pictures, and as long as the photos and PII remained online, the threats, unwanted contacts and harm to reputation would continue to flow. (See *Peniston, supra*, 242 Cal.App.2d at pp. 722-724.)

Rather than discuss or even cite *Peniston*, appellant relies on *Cross v. Cooper, supra*, 197 Cal.App.4th 357 for the proposition that there could be no disclosure of a secret when the images were publicly available (on appellant's website) for all to see. (AOB 52-53.) However, that case does not assist appellant. In *Cross*, a landlord sued her tenants for breach of contract and a variety of torts based on the allegations that the tenants threatened to disclose to prospective buyers that a registered sex offender lived nearby unless the landlord agreed to waive one month's rent. (*Id.* at pp. 365-366.) The tenant moved to dismiss under the anti-SLAPP (Strategic Lawsuit Against Public Participation) provisions of Code of Civil Procedure section 425.16. The trial court denied the motion, but the Court of Appeal reversed. In order to survive the anti-SLAPP motion, the landlord had to conclusively establish that the tenant's acts were illegal as a matter of law and, therefore, not entitled to anti-SLAPP protection. The Court of Appeal held the landlord could not satisfy this burden because the record established that most, if not all, elements of such an offense are "contested issues of fact." (*Cross, supra*, 197 Cal.App.4th at p. 388.) Relying on all the circumstances, including the fact that the location of the sex offenders was both publicly available and, in any event, the landlord was required to disclose this information before any sale, the Court of Appeal reasoned that the record did not "conclusively prove that the location of the offender was a matter so unfavorable to [the landlord's] interests or that she so feared its disclosure. . . ." (*Ibid.*)

Thus, contrary to appellant's position, the *Cross* court did not hold that information publicly available on a website cannot constitute a secret for purposes of extortion. Instead, the court simply held that the purportedly extorted party (i.e., the landlord) could not establish that the tenants' actions necessarily constituted extortion as a matter of law because the resolution of this issue depended on the facts of the case. Here, the roles are

reversed, and this Court must presume in support of the judgment the existence of every fact the trier could reasonably deduce from the evidence. (*People v. Kraft, supra*, 23 Cal.4th at p. 1053.) “The elements of threat and fear being questions of fact for the jury’s determination, its finding in that regard will not be set aside where the evidence, as in the present case, supports its conclusion.” (*People v. Oppenheimer, supra*, 209 Cal.App.2d at p. 424.)

Indeed, the *Cross* court specifically cited *Peniston* and *Lavine*, reiterating the long-established principle that for purposes of extortion, ““The “secret” referred to in the statute is a matter “unknown to the general public, or to some particular part thereof which might be interested in obtaining knowledge of the secret. . . .”” (*Cross, supra*, 197 Cal.App.4th at p. 387, italics added.) Under this definition, public information may still be a secret as long as there is some segment of the population that is unaware of the information. In light of *Cross*’s own duty to disclose this very information, *Cross* failed to show that it was not a contested question of fact whether the location of the sex offender was a secret. (*Id.* at p. 388.)

But even if the widespread disclosure meant that appellant could not “expose” a “secret,” the continued posting of the pictures on the Internet threatened to impute a “disgrace” under section 519, subdivision (3). Unlike subdivision (4), which proscribes exposure of a secret, the language of subdivision (3) may be satisfied alternatively either by acts that “expose” or acts that “impute” a disgrace. By drawing this distinction, the Legislature presumably meant to proscribe acts that attribute a disgrace, even once that disgrace has already been exposed. And this distinction makes sense: a person’s reputation may be harmed anew with each fresh suggestion of disgrace, even if that disgrace is not a secret and even if it has previously been exposed. (Cf. *Melvin v. Reid, supra*, 112 Cal.App. at p. 292 [publication of “unsavory incidents” in woman’s past life, after she had

reformed, coupled with her true name, violated her right of privacy].) As the testimony in the instant case amply revealed, as long as the photos remained on the Internet, the victims could not begin to mend their reputations. Any requirement that the qualifying disgrace not be known or previously revealed would collapse the distinction between “secret” and “disgrace,” and blur the difference between the alternative elements of “expos[ing]” and “imput[ing].”¹⁶

Relying on the Ninth Circuit’s interpretation of California law in *Levitt v. Yelp! Inc.* (9th Cir. 2014) 765 F.3d 1123 (*Yelp!*), appellant alternatively contends that as an interactive computer service provider he was “under no legal obligation to remove the postings submitted to the website by third parties, even when those postings are negative in nature.” (AOB 50.) Appellant maintains that because he could have refused to remove the offending content, offering to remove the content for a fee could not have constituted extortion. (AOB 50.) But *Yelp!* is distinguishable because the instant case does not simply involve “negative” information or reviews; the victims here had a pre-existing right to have their photos and other personal information removed. Further, appellant misapprehends California law and the Ninth Circuit’s interpretation of that law is neither controlling nor persuasive.

In *Yelp!*, several business owners alleged that Yelp!, Inc., which provides an online forum for users to rate and express opinions about

¹⁶ For similar reasons, continued exposure of the victims’ photos and personal identifying information threatened the victims with an “unlawful injury to the person or property” under section 519, subdivision (1). There is no requirement of an “exposure” under this provision. Instead, the victims continued to suffer harm as long as Internet trolls were able to contact them using the personal data that appellant provided. The jury, however, was not instructed on this theory. (2CT 379.)

businesses, created negative reviews of their businesses and manipulated review and ratings content to induce them to purchase advertising. For instance, one small business owner alleged that two days after he declined to purchase advertising from Yelp!, several positive reviews disappeared from the Yelp! website and his overall rating declined from 4.5 stars to 3 stars. (*Yelp!*, *supra*, 765 F.3d at p. 1127.) The Ninth Circuit held that the allegations failed to state a claim for economic extortion under either the Hobbs Act (18 U.S.C. § 1951(b)(2)) or Penal Code sections 518 and 519. (*Id.* at p. 1134.) The court concluded that to state a claim under the Hobbs Act and California law, “a litigant must demonstrate either that he had a pre-existing right to be free from the threatened harm, or that the defendant had no right to seek payment for the service offered.” (*Id.* at p. 1133.) Applying these requirements, the court concluded that the businesses had no pre-existing right to have positive reviews appear on the Yelp! website, and therefore, they could not be extorted by Yelp!’s removal of those positive reviews or manipulation of the order of the reviews. (*Id.* at pp. 1133-1134.)

At the outset, it is not clear that California law is entirely co-extensive with federal law. The *Yelp!* court was apparently relying solely on section 519, subdivision (1), which proscribes a threat to do an “unlawful injury to the person or property” of the victim. (*Yelp!*, *supra*, 765 F.3d at pp. 1132-1133.) The court did not grapple with exposure of a secret or imputation of a disgrace or deformity under section 519, subdivisions (3) and (4), which contain no similar limitation of only applying to “unlawful” revelations. For instance, in *Peniston*, which involved the threatened exposure of a secret under subdivision (3), there was no discussion of any requirement that the victim have “a pre-existing right to be free from the threatened harm,” as the Ninth Circuit required in *Yelp!*, 765 F.3d at page 1133. Nor did the facts in *Peniston* reveal the victim had such a pre-existing right

based on photos that were otherwise widely exhibited. (*Peniston*, 242 Cal.App.2d at pp. 722-723.) The threat of exposure, and the fear that it engendered, were sufficient by themselves to state a claim. (*Id.* at p. 722.)

Contrary to the pre-existing right test announced in *Yelp!*, our state Supreme Court has recognized that threats to do otherwise legal action can, in some circumstances, give rise to claims of extortion: “Extortion has been characterized as a paradoxical crime in that it criminalizes the making of threats that, in and of themselves, may not be illegal. “[I]n many blackmail cases the threat is to do something in itself perfectly legal, but that threat nevertheless becomes illegal when coupled with a demand for money.” (*Flatley v. Mauro*, *supra*, 39 Cal.4th at p. 326, quoting *Philippine Export & Foreign Loan Guarantee Corp. v. Chuidian* (1990) 218 Cal.App.3d 1058, 1079.) Obviously, the California Supreme Court’s interpretation of California is controlling, not the Ninth Circuit’s. (*People v. Crittenden* (1994) 9 Cal.4th 83, 120, fn. 3; *Howard Contracting, Inc. v. G.A. MacDonald Construction Co.* (1998) 71 Cal.App.4th 38, 52 [“federal decisional authority is neither binding nor controlling in matters involving state law”].)

In any event, even if *Yelp!* were correct, there was more than adequate evidence of a pre-existing legal duty in the present case. The victims here had a right not to have their personal identifying information made public on appellant’s website. (§§ 530.5, 530.55.) This was not, as in the case of *Yelp!*, simply a manipulation of negative reviews; the victims here had a right of privacy over their personal information and photographs that appellant published on his website.

Appellant’s assertion that he could have legally declined to remove the content because he was immune under the CDA as an interactive service provider (AOB 50) is incorrect for the reasons discussed in Argument I, *infra*. The present case is distinguishable from *Yelp!* because

appellant actively developed content by requiring users to post the victims' PII. He did not simply create a forum for users to post comments, good or bad, about a victim. Instead, he required that the postings contain specific PII content and that content violated the victims' right of privacy. Moreover, as previously discussed, appellant did not simply fail to remove the offending images and data; he actively developed and encouraged that information through the required fields of his website. Accordingly, there was sufficient evidence of extortion even under the Ninth Circuit's tests in *Yelp!*.

Finally, even if appellant could show there were insufficient facts to support either of the two theories of extortion, the jury would not have relied on any such inadequate theory. (*People v. Guiton, supra*, 4 Cal.4th at p. 1131.)

III. APPELLANT INVITED ANY ERROR REGARDING THE CACI INSTRUCTIONS HE REQUESTED; IN ANY EVENT, THE INSTRUCTIONS, WHEN CONSTRUED AS A WHOLE, REQUIRED THE JURY TO DETERMINE EVERY ELEMENT BEYOND A REASONABLE DOUBT

The unauthorized use of PII under section 530.5, subdivision (a), required the People to show, among other things, that appellant willfully used PII for an "unlawful purpose." (2CT 381.) As previously noted, the People proceeded on three separate theories to show an unlawful purpose: (i) violation of section 653m; (ii) public disclosure of private facts; and (iii) intrusion into private affairs. (2CT 385.) The requirements of the latter two theories were defined in separate instructions under CACI 1800 and 1801. (2 CT 387-388.) Appellant argues the trial court erred in giving the CACI instructions, because those apply to civil litigation and the standard applied to a civil wrong is lower than the standard of proof beyond a reasonable doubt. (AOB 54-59.) But appellant invited any error by requesting the very instructions he now challenges. In any event, he cannot demonstrate error

because the instructions, construed as a whole, unambiguously required the jury to find all elements, including those set forth in the two CACI instructions, beyond a reasonable doubt.

At the outset, appellant invited any error. (See *People v. Lucero* (2000) 23 Cal.4th 692, 723, [“The doctrine of invited error bars a defendant from challenging an instruction given by the trial court when the defendant has made a ‘conscious and deliberate tactical choice’ to ‘request’ the instruction”].) Contrary to his current assertions (AOB 54), it was appellant who specifically requested that the trial court instruct the jury with CACI 1800 and 1801. (7RT 996-998.) The People had proposed instructing the jury with BAJI 7.20 and 7.21, and opposed appellant’s suggested instructions. (7RT 996, 1001-1004.) The court overruled the People’s objection and gave appellant’s requested instructions. (7RT 1004-1005.) The defense had tactical reasons for making this request. (7RT 998-999.) As defense counsel noted, CACI 1800 gave “something for the defense to argue” regarding whether the victims had a reasonable expectation of privacy. (7RT 1003.) The People, on the other hand, favored clarifying that the expectation must be assessed in reference to the identity of the intruder and the nature of the claimed violation. (7RT 1004.) The trial court concluded that these were factors for the People to argue. (7RT 1004-1005.) The defense submitted CACI 1801 in order to be consistent. (7RT 1006.) In light of these facts, appellant made a “conscious and deliberate tactical choice” to request the instructions he now challenges, and his claim is procedurally barred on appeal. (See, e.g., *People v. Turner* (2004) 34 Cal.4th 406, 434 [finding invited error where defendant proposed an instruction, the People objected, and both parties subsequently agreed to the language to be included]; *People v. Seaton* (2001) 26 Cal.4th 598, 667-668 [purported defects in standard instructions not reviewable where defendant requested those instructions]; *People v. Weaver* (2001) 26 Cal.4th 876, 969-

970 [claim barred where defense counsel requested challenged instruction].)

Even assuming appellant's claim were preserved, it lacks merit. In order to demonstrate jury instructions are misleading, a defendant must prove a reasonable likelihood the jury misunderstood the instructions construed as a whole. (*People v. Cain* (1995) 10 Cal.4th 1, 36, 40; *People v. Kelly* (1992) 1 Cal.4th 495, 525; *People v. Price* (1991) 1 Cal.4th 324, 446; *People v. Jenkins* (1994) 29 Cal.App.4th 287, 297.) “““The absence of an essential element in one instruction may be supplied by another or cured in light of the instructions as a whole.””” (*People v. Castillo* (1997) 16 Cal.4th 1009, 1016; *People v. Van Winkle* (1999) 75 Cal.App.4th 133, 147.) The reviewing court must assume the jurors were intelligent persons and capable of understanding and correlating all jury admonitions and instructions which were given. (*People v. Mills* (1991) 1 Cal.App.4th 898, 918.) As the United States Supreme Court has commented:

Jurors do not sit in solitary isolation booths parsing instructions for subtle shades of meaning in the same way that lawyers might. Differences among them in interpretations of instructions may be thrashed out in the deliberative process with commonsense understanding of the instructions in light of all that has happened at trial likely to prevail over technical hairsplitting

(*Boyde v. California* (1990) 494 U.S. 370, 380-381.) “*Boyde*. . . mandates that the whole context of the trial be considered.” (*Brown v. Payton* (2005) 544 U.S. 133, 144.)

Appellant fails to abide by these principles. Here, the court expressly instructed the jury regarding the requirements of proof beyond a reasonable doubt under CALCRIM No. 220. That instruction informed the jury, among other things, that “A defendant in a criminal case is presumed to be innocent. This presumption requires that the People prove a defendant guilty beyond a reasonable doubt. *Whenever I tell you the People must*

prove something, I mean they must prove it beyond a reasonable doubt.” (2CT 370, italics added.) The court reiterated this principle by giving CALCRIM No. 224, which stated in relevant part that “Before you may rely on circumstantial evidence to conclude that a fact necessary to find the defendant guilty has been proved, you must be convinced that the People have proved each fact essential to that conclusion beyond a reasonable doubt.” (2CT 359.) The court also gave a similar instruction regarding circumstantial evidence used to show intent. (CALCRIM No. 225; 2CT 392.)

Regarding section 530.5 in particular, the trial court instructed the jury that to find appellant guilty of that offense, the People had to prove the following three elements:

1. The defendant willfully obtained someone else’s personal identifying information;
2. The defendant willfully used that information for an unlawful purpose

AND

3. The defendant used the information without the consent of the person whose identifying information he was using.

(2CT 381.) Finally, CALCRIM No. 251 underscored that the charged crimes required proof of the union, or joint operation, of act and wrongful intent; to find appellant guilty, he had to not only commit the prohibited act, but do so with a specific intent. (2CT 389.)

Appellant points to nothing in the language of CACI 1800¹⁷ or 1801¹⁸ that suggested the burden of proof was anything less than proof beyond a

¹⁷ CACI 1800, as adapted, stated as follows:
Intrusion Into Private Affairs

(continued...)

(...continued)

An unlawful purpose required for the unauthorized use of personal identifying information as charged in several counts may also be based upon a claim of invasion of privacy by intrusion into private affairs. The essential elements of this claim are:

1. That victim had a reasonable expectation of privacy in the photographs and other personal identifying information;
2. That the defendant intentionally intruded into the solitude, seclusion or private affairs of the victim;
3. That the defendant's intrusion would be highly offensive to a reasonable person;
4. That victim was harmed; and
5. That defendant's conduct was a substantial factor in causing the victim's harm.

In deciding whether the victim had a reasonable expectation of privacy in the photographs or other personal identifying information, you should consider, among other factors, the following:

- (a) The identity of the defendant
- (b) The extent to which other persons had access to the photographs and other personal identifying information and could see or hear the victim and
- (c) The means by which the intrusion occurred.

In deciding whether an intrusion is highly offensive to a reasonable person, you should consider, among other factors, the following:

- (a) The extent of the intrusion;
- (b) The defendant's motives and goals; and
- (c) The setting in which the intrusion occurred.

(2 CT 387.)

¹⁸ CACI 1801, as adapted, stated as follows:
Public Disclosure of Private Facts

An unlawful purpose required for the unauthorized use of personal identifying information as charged in several counts may also be based upon a claim of invasion of privacy by public disclosure of private facts.

(continued...)

reasonable doubt. Instead, he relies on the generalized notion that “the standard applied to a civil wrong is lower than beyond a reasonable doubt as is applied to a criminal offense and all elements of that offense.” (AOB 55.) But he ignores the fact that the instructions here, construed as a whole, unambiguously required the jury to find appellant guilty of all elements beyond a reasonable doubt. Notably, appellant does not even mention CALCRIM No. 220. Nor does he suggest that either counsel intimated that the standard for proving an intrusion into private affairs or public disclosure

(...continued)

1. That the defendant publicized private information concerning the victim;
2. That a reasonable person in the victim’s position would consider the publicity highly offensive;
3. That the defendant knew, or acted with reckless disregard of the fact, that a reasonable person in victim’s position would consider the publicity highly offensive;
4. That the private information was not of legitimate public concern or did not have a substantial connection to a matter of legitimate public concern;
5. That the victim was harmed; and
6. That the defendant’s conduct was a substantial factor in causing the victim’s harm.

In deciding whether the information was a matter of legitimate public concern, you should consider, among other factors, the following:

- (a) The social value of the information;
- (b) The extent of the intrusion into victim’s privacy;
- (c) Whether the victim consented to the publicity explicitly or by voluntarily seeking public attention or a public office;

In deciding whether the defendant publicized the information, you should determine whether it was made public either by communicating it to the public at large or to so many people that the information was substantially certain to become public knowledge.

(2CT 388.)

of private facts could be based on a mere preponderance of evidence or anything less than proof beyond a reasonable doubt

In a final and unsupported sentence, appellant asserts that “The use of elements of civil wrongs to establish criminal liability was error.” (AOB 58.) But at least one court has rejected a similar contention. (*In re Rolando S.*, *supra*, 197 Cal.App.4th at p. 942.) In *Rolando S.*, the defendant used the victim’s email password and account to gain access to her Facebook account, where he posted prurient messages in her name. (*Id.* at p. 939.) On appeal, the defendant argued that while he may have defamed the victim, civil torts do not constitute an “unlawful purpose” under section 530.5, subdivision (a). Rejecting this assertion, the Court of Appeal held that intentional civil torts, such as libel, constitute an “unlawful purpose” under that provision. (*Id.* at p. 942.) The court reached this conclusion after determining, based on its exhaustive examination of the legislative history behind section 530.5 and its amendments, that “The Legislature clearly intended to greatly expand the scope of unlawful conduct underlying the identity theft offense.” (*Id.* at p. 945.) The *Rolando S.* court observed that the term “unlawful” includes wrongful conduct that is not criminal, noting that “an act is ‘unlawful. . . if it is proscribed by some constitutional, statutory, regulatory, common law, or other determinable legal standard.’” (*Id.* at p. 946, quoting *Korea Supply Co. v. Lockheed Martin Corp.* (2003) 29 Cal.4th 1134, 1159.)

Appellant does not discuss this portion of *Rolando S.* (cf. AOB 39 discussing *Rolando S.*’s treatment of the “willfully” requirement), or otherwise give this Court any reason to distinguish the torts at issue here. While the holding in *Rolando S.* was limited to intentional torts, such as the libel challenged in that case, nothing in its reasoning or the legislative history suggests such a limitation. Although intrusion into private affairs is an intentional tort (*Sanders, supra*, 20 Cal.4th at p. 926 [intentional

intrusion required]; CACI 1800; 2CT 387), public disclosure of private facts requires only that the defendant knew, or acted with reckless disregard of, the fact that a reasonable person in the victim's position would consider the publicity highly offensive (CACI 1801; 2CT 388). This satisfies the requirement of *Rolando S.* of conduct that is "proscribed by some . . . common law, or other determinable legal standard." (*In re Rolando S.*, *supra*, 197 Cal.App.4th at p. 946.) Moreover, in any event, the jury here was instructed that in order to be guilty of violating section 530.5, subdivision (a), the defendant had to "willfully" use the information for an unlawful purpose. (2CT 381.) The jury was further instructed that he had to commit the act with a specific intent. (2CT 389.) Thus, as instructed, the jury nonetheless specifically had to find that appellant acted with the requisite intent.

CONCLUSION

Accordingly, for the reasons stated above, respondent respectfully requests that this Court affirm the judgment.

Dated: February 4, 2016

Respectfully submitted,

KAMALA D. HARRIS
Attorney General of California
GERALD A. ENGLER
Chief Assistant Attorney General
JULIE L. GARLAND
Senior Assistant Attorney General
ERIC A. SWENSON
Supervising Deputy Attorney General
JUNICHI P. SEMITSU
Deputy Attorney General
GARRETT A. GORLITSKY
Deputy Attorney General



STEVE OETTING
Deputy Solicitor General
Attorneys for Plaintiff and Respondent

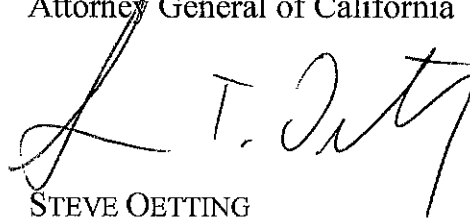
SO:lb
SD2015801333
71163154.doc

CERTIFICATE OF COMPLIANCE

I certify that the attached RESPONDENT'S BRIEF uses a 13-point Times New Roman font and contains 19,852 words.

Dated: February 4, 2016

KAMALA D. HARRIS
Attorney General of California

A handwritten signature in black ink, appearing to read "S. T. Oetting", is written over the printed name of Steve Oetting.

STEVE OETTING
Supervising Deputy Attorney General
Attorneys for Plaintiff and Respondent

DECLARATION OF SERVICE BY U.S. MAIL & ELECTRONIC SERVICE

Case Name: **People v. Bollaert**

No.: **D067863**

I declare: I am employed in the Office of the Attorney General, which is the office of a member of the California State Bar, at which member's direction this service is made. I am 18 years of age or older and not a party to this matter. I am familiar with the business practice at the Office of the Attorney General for collection and processing of correspondence for mailing with the United States Postal Service. In accordance with that practice, correspondence placed in the internal mail collection system at the Office of the Attorney General is deposited with the United States Postal Service that same day in the ordinary course of business. The Office of the Attorney General's eService address is AGSD.DAService@doj.ca.gov.

On February 4, 2016, I served the attached **RESPONDENT'S BRIEF** by placing a true copy thereof enclosed in a sealed envelope with postage thereon fully prepaid, in the internal mail collection system at the Office of the Attorney General at 600 West Broadway, Suite 1800, P.O. Box 85266, San Diego, CA 92186-5266, addressed as follows:

Electronic Service Only:

Patrick J. Hennessey, Jr.

Attorney at Law

2356 Moore St., Ste. 201

San Diego, CA 92110

ADI Panel Attorney for Appellant

pjhjr@hotmail.com

Electronic Service Only:

Appellate Defenders, Inc.

555 West Beech Street, Suite 300

San Diego, CA 92101

Clerk, Criminal Appeals – FOR:

Honorable David M. Gill, Judge

San Diego County Superior Court

220 West Broadway

San Diego, CA 92101-3409

Electronic Service Only:

The Honorable Bonnie M. Dumanis

District Attorney – Attn: Appeals

San Diego County District Attorney's

Office

330 West Broadway, Suite 1320

San Diego, CA 92101

Additionally, in compliance with California Rules of Court, rules 2.251(i)(1)(A)-(D) and 8.71(f)(1)(A)-(D), and by 5:00 p.m. on the close of business day, I electronically served a copy of the above document on February 4, 2016, to the following.

eservice-criminal@adi-sandiego.com

Appellate Defenders, Inc.'s

pjhjr@hotmail.com

Appellant's Attorney

da.appellate@sdcda.org

San Diego District Attorney's Office

I declare under penalty of perjury under the laws of the State of California the foregoing is true and correct and that this declaration was executed on February 4, 2016, at San Diego, California.

L. Blume

Declarant



Signature